Octavian Stănășilă

NOȚIUNI ȘI TEHNICI DE MATEMATICĂ DISCRETĂ

EDITURA ȘTIINȚIFICĂ ȘI ENCICLOPEDICĂ

NOȚIUNI ȘI TEHNICI DE MATEMATICĂ DISCRETĂ

O. STĂNĂȘILĂ

NOȚIUNI ȘI TEHNICI DE MATEMATICĂ DISCRETĂ

Editura Științifică și Enciclopedică
București, 1985

Coperta de Gh. G. Marinescu

Editura Științifică și Enciclopedică
București, 1985

PREFAȚĂ

O parte consistentă a matematicii este identificată cu calculul, în diversele lui ipostaze — calcul algebric, calcul logic, calcul diferențial și integral, geometrie analitică, analiză numerică etc. Tehnicile moderne de comandă și de prelucrare a datelor au impus o analiză profundă a însuși conceptului general de calcul. Matematica discretă este strîns legată de această analiză, precum și de studiul sistematic al ordonării și organizării diverselor structuri. În acest sens, au fost elaborate multe noțiuni și construcții specifice fenomenelor „discrete", finite sau recurent numărabile, bazate pe exploatarea prin excelență a structurilor algebrice și de ordine, pornind de la obiecte matematice esențiale — numere, seturi de numere, relații, funcții, predicate, operații etc. Bineînțeles, matematica este doar una și nu se poate vorbi de o nouă matematică — cea discretă.

Denumirea de matematică discretă sugerează tacit convenția de a renunța oarecum la utilizarea noțiunii de limită și la întreg eșafodajul bazat pe aceasta (topologie, varietăți, derivate, integrale, ecuații diferențiale, analiză complexă, analiză funcțională etc.). Utilizarea mai restrînsă a operației atît de fecunde a trecerii la limită ar putea însemna o anumită simplificare pînă la sărăcire de conținut. În realitate, matematica discretă este un domeniu bine circumscris, bogat în rezultate profunde și avînd în fond puternice legături cu matematica entităților continue, dezvoltări spectaculoase ale acesteia fiind cuplate cu puterea crescîndă de calcul. În același timp, structurile discrete joacă un rol decisiv în multiple arii ale științei și tehnologiei moderne și se poate afirma că discretizarea și cuantizarea au devenit instrumente esențiale, universale de investigație, depășind propriu-zis pragul matematicii.

În această lucrare am selectat cîteva capitole de matematică discretă, care conțin teoreme fundamentale, însoțite de aplicații pe care le-am socotit semnificative, luate îndeosebi din domeniul calculatoristicii. Noțiunile de operație, algoritm, numărare, cardinal, relație de ordine, graf, arbore, automat, limbaj, funcție parțial recur-

sivă, limbaj recunoscut, limbaj raţional, organigramă, program etc., obţinute prin abstractizare şi lărgire progresivă a conceptelor de mulţime, funcţie, număr cardinal, număr ordinal, şir finit de obiecte etc. sînt indispensabile în multe descrieri matematice, ca şi în manipulări directe sau recurente de simboluri supuse la reguli prestabilite. În acelaşi timp, ele sînt intim legate de entităţile recunoscute de maşini care au un număr finit de stări. Este neîndoielnic că odată cu rezolvarea problemelor ştiinţifice strict numerice, calculatorul este tot mai implicat în probleme nenumerice în care datele au „structuri atomice" constînd din seturi ordonate de biţi sau caractere.

Acestea sînt cîteva argumente în favoarea tematicii propuse, consacrată în principal prezentării unor noţiuni de bază. Nu am abordat unele capitole de matematică discretă alcătuind teritorii relativ independente — combinatorică, metode probabiliste discrete, logică multivalentă şi mulţimi vagi, prelucrarea semnalelor şi recunoaşterea formelor, inteligenţă artificială, învăţare şi teoria modelelor, logica acţiunii umane, analiza dualităţii dintre idee şi calcul sau analiza limitelor algoritmicului etc. (pentru aceasta trimitem la [6], [9], [13], [30,] [34], [37], [42], [56] etc.).

Am scris această carte din dorinţa de a contribui la asimilarea unor concepte şi tehnici care interesează cercuri largi de cititori, extinzînd lucrarea *Elemente de matematică discretă* [50], elaborată pe baza unor note de curs; deosebit de utile mi-au fost de asemenea discuţiile cu cadre didactice şi studenţi de la facultăţile de automatică şi electronică din Bucureşti, îndeosebi cele purtate în cadrul seminarului Matematică şi/sau programare. Un cuvînt de mulţumire am şi pentru cei care au sprijinit apariţia acestei lucrări.

iunie 1984 **O. Stănăşilă**

NOTAȚII

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ — sistemele de numere naturale, întregi, raționale, reale, complexe
$\emptyset$ — mulțimea vidă
$\mathbf{1}$ — mulțime formată dintr-un singur element
$\mathbb{B}$ — codul binar (mulțime având două elemente, notate 0 și 1 sau A și F)
$\leftrightarrow$ — dacă și numai dacă
$\forall$ — oricare ar fi ; $\exists$ — există cel puțin un ; $\exists !$ — există și este unic
$A \subset B$ — incluziune ; $A \subsetneq B$ — incluziune strictă
$A \sim B$ — mulțimile A și B sînt echipotente
$\mathcal{P}(A)$ — mulțimea părților lui A
$|M|$ — cardinalul lui M ; $|\mathcal{A}|$ — comportarea automatului $\mathcal{A}$
$\blacksquare$ — sfîrșitul demonstrației
$f : A \to B$, $x \mapsto f(x)$ reprezintă o funcție (notată f) definită pe mulțimea A cu valorile în B ; oricărui element $x \in A$ i se asociază elementul $f(x)$ din B ; B^A — mulțimea tuturor funcțiilor $f : A \to B$
$S_n = \{x \in \mathbb{N} \mid x < n\} = \{0, 1, \ldots, n-1\}$ pentru orice $n \in \mathbb{N}$ ($S_0 = \emptyset$, $S_1 = \mathbf{1}$, $S_2 \sim \mathbb{B}$)
Rel S — mulțimea relațiilor binare pe S ; **Rel** — categoria relațiilor
X^* — dicționarul alfabetului X
Rat (Σ) (resp. Rec (Σ)) — mulțimea elementelor raționale (resp. recognoscibile) dintr-un monoid complet ordonat $W (\Sigma \subset W)$.

TABLA DE MATERII

Prefață 5

Capitolul 1 INIȚIALIZARE ȘI DINAMICĂ 9

§ 1.1. Relații și interpretări sistemice 9
§ 1.2. Dinamici Peano 20
§ 1.3. Relații, predicate și operații algebrice n-are ($n \in \mathbb{N}$) 37
§ 1.4. Dicționarul unui alfabet; dinamici peste o mulțime oarecare . . . 45
§ 1.5. Serii formale și aplicații în studiul unor sisteme discrete 62

Capitolul 2 FINITUDINE ȘI NUMĂRARE 78

§ 2.1. Mulțimi finite 78
§ 2.2. Cardinalitate. 88
§ 2.3. Numărări 91
§ 2.4. Structuri algebrice pe mulțimi finite 97

Capitolul 3 STRUCTURI ARBORESCENTE ȘI CALCULABILITATE 109

§ 3.1. Grafuri și categorii. 109
§ 3.2. Elemente de algebră universală 121
§ 3.3. Arbori etichetați 131
§ 3.4. Automate; automate-arbore. 136
§ 3.5. Calculabilitate 143

Capitolul 4 ORDINE, DINAMICĂ DISCRETĂ ȘI PROGRAMARE RAȚIONALĂ 160

§ 4.1. Latici complete. Sisteme de închidere 160
§ 4.2. Operatori izotoni și supratopologii 170
§ 4.3. Puncte fixe ale operatorilor izotoni 178
§ 4.4. Monoizi complet ordonați 184
§ 4.5. O generalizare a teoremei lui Kleene. Aplicații în programare . . . 187

Bibliografie 199

Indice de noțiuni 203

CAPITOLUL 1

INIȚIALIZARE ȘI DINAMICĂ

Introducere

În acest capitol vom reaminti mai întîi conceptele de relație, funcție, operație însoțite de exemple și interpretări sistemice. De asemenea, vom da unele construcții ansambliste utilizate în mod curent, fixînd totodată terminologia și notațiile.

Obiectele matematice esențiale sînt : numerele, seturile de numere și funcțiile, însă există resurse inepuizabile de îmbogățire a cunoașterii cu entități aflate sub incidența instrumentului matematic. Vom insista asupra prezentării mulțimii $\mathbb{N}$ a numerelor naturale deoarece ea redă ideea de discret constructiv și prefigurează conceptul de automat, definit esențialmente prin dinamica de trecere de la o stare la alta și prin inițializare (starea inițială). În acest context unele rezultate „subînțelese" capătă o importanță principială în legătură cu instrumentul atît de puternic și plin de resurse pe care îl reprezintă inducția matematică.

În ultimul paragraf vom studia în detaliu X-dinamicile, care sînt strîns legate de dicționarul unui alfabet X și sînt utilizate în multe construcții matematice de natură discretă, îndeosebi algoritmice.

§ 1.1. RELAȚII ȘI INTERPRETĂRI SISTEMICE

Notații

Vom considera că noțiunile de mulțime, element, obiect, parte (submulțime), clasă etc. sînt primare, situîndu-ne în cadrul teoriei neformalizate a mulțimilor. Colecțiile de obiecte sînt întîlnite în orice descriere, astfel că nu este întîmplător că orice discurs matematic utilizează limbajul mulțimilor.

Vom nota cu $\emptyset$ mulțimea vidă și cu $\mathbb{1}$ o mulțime avînd un singur element (fixat și notat simbolic cu λ), deci $\mathbb{1} = \{\lambda\}$. Notînd cu **F** (resp. **A**) simbolul falsului (resp. al adevărului), mulțimea

$$\mathbb{B} = \{\mathbf{F}, \mathbf{A}\}$$

avînd două elemente distincte, se numește *codul binar* (sau mulțimea lui G. Boole, 1815-1864). Adeseori se notează 0 în loc de **F**

și 1 în loc de A, punînd $\mathbb{B} = \{0, 1\}$; dar 0 și 1 nu reprezintă aici numere naturale.

Convenim să fixăm o clasă de mulțimi $\mathfrak{U}$ (numită *univers*) care să conțină

$$\emptyset,\ \mathbb{B},\ \mathbb{N} = \{0, 1, 2, \ldots, n, \ldots\},\ \mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\},$$

$$\mathbb{Q} \quad \left\{\frac{p}{q} \,\middle|\, p, q \in \mathbb{Z},\ q \neq 0\right\},\ \mathbb{R}$$

și astfel încît toate mulțimile considerate în continuare să fie părți ale unor mulțimi din $\mathfrak{U}$ sau să se obțină din acestea prin operații de reuniune, intersecție, trecere la complementară, produs cartezian etc.

Pentru o mulțime M se va nota cu $\mathfrak{p}(M)$ mulțimea tuturor părților lui M, adică $\mathfrak{p}(M) = \{N \mid N \subset M\}$. Evident, $M \in \mathfrak{p}(M)$, $\emptyset \in \mathfrak{p}(M)$.

Exemple. $\mathfrak{p}(0) = \{0\}$, $\mathfrak{p}(\emptyset) = \{0, \emptyset\}$, $\mathfrak{p}(\mathbb{B}) = \{0, \{0\}, \{1\}, \mathbb{B}\}$.

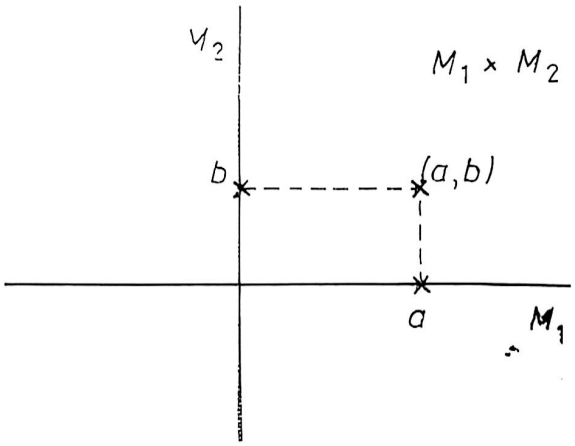


Fig. 1.1

Dacă M_1, M_2 sînt două mulțimi, *produsul lor cartezian* este mulțimea $M_1 \times M_2$ a tuturor perechilor ordonate (a, b) cu $a \in M_1$, $b \in M_2$ (perechea ordonată (a, b) este o entitate distinctă de mulțimea $\{a, b\}$). Dacă $M_1 = M_2 = M$, atunci se scrie M^2 în loc de $M \times M$. În cazul cînd M_1 sau M_2 este vidă, atunci $M_1 \times M_2 = \emptyset$. *Reuniunea disjunctă* (numită și *suma*) mulțimilor M_1, M_2 este prin definiție

$$M_1 + M_2 = (\{0\} \times M_1) \cup (\{1\} \times M_2).$$

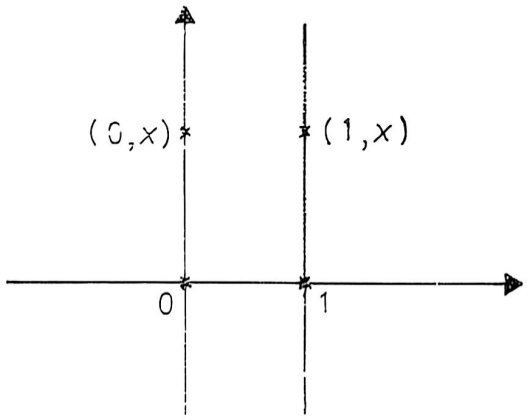


Fig. 1.2

Exemple. 1) Fie $M_1 = \{a, b\}$, $M_2 = \{1, 2, 3\}$. Atunci $M_1 \times M_2 = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$ și $M_1 + M_2 = \{(0, a), (0, b), (1, 1), (1, 2), (1, 3)\}$.

2) Fie $M_1 = M_2 = \mathbb{R}$ (mulțimea numerelor reale); atunci produsul cartezian $M_1 \times M_2 = \mathbb{R}^2$ este identificat cu planul geometriei analitice a lui R. Descartes (1596-1650), iar suma $M_1 + M_2$ este reuniunea mulțimilor disjuncte $\{(0, x) \mid x \in \mathbb{R}\}$, $\{(1, x) \mid x \in \mathbb{R}\}$.

Relații

Conceptul de relație este fundamental pentru că el generalizează multe exemple concrete — relația de inegalitate „$\leqslant$" între numere, relația „mai ieftin" în comerț, relația de incluziune între mulțimi, relații de asociere, de dependență funcțională etc.

Vom începe cu un exemplu simplu. Să presupunem că într-o bibliotecă se păstrează diverse lucrări — cărți, manuscrise etc. formînd o mulțime de obiecte $M = \{l_1, l_2, \ldots, l_p\}$. Pentru fixarea locului fiecărei lucrări se folosesc unul sau mai mulți descriptori dintr-o mulțime $N = \{d_1, d_2, \ldots, d_q\}$. Legătura dintre lucrări și descriptorii lor este bine definită dacă se precizează pentru fiecare lucrare $l_i \in M$, $1 \leqslant i \leqslant p$, setul de descriptori corespunzător $\{d_1^{(i)}, \ldots, d_{r_i}^{(i)}\} \subset N$. În acest mod este pusă în evidență o colecție de perechi de elemente, anume

$$\{(l_1, d_1^{(1)}), \ldots, (l_1, d_{r_1}^{(1)}), (l_2, d_1^{(2)}), \ldots, (l_p, d_{r_p}^{(p)})\} \subset M \times N.$$

Fiind date două mulțimi M și N, a stabili o relație (binară) între elementele lor, revine la a evidenția o colecție de perechi (a, b) de elemente aflate în relația respectivă, cu $a \in M$, $b \in N$. Nu este exclus cazul $M = N$.

Aceste considerații pregătesc noțiunea generală următoare.

DEFINIȚIA 1.1. Se numește *relație binară* (sau *corespondență*) de la M la N orice triplet ordonat

$$\rho = (M, N, R),$$

unde M și N sînt mulțimi, iar R este o submulțime a lui $M \times N$.

Se mai scrie atunci $\rho : M \to N$; R se numește *graficul* relației ρ, M este *sursa*, iar N *cosursa* lui ρ. Dacă $x \in M$, $y \in N$ și $(x, y) \in R$, atunci se scrie

$$x \rho y \text{ (sau } xRy \text{ sau } x \overset{R}{\longrightarrow} y),$$

ceea ce se citește astfel: x este în relația ρ (sau R) cu y.

În situații concrete, relațiile sînt notate prin simboluri specifice ($\leqslant$, $\subset$, : etc.) și nu prin litere.

Dacă $x \in M$ este un element fixat, atunci se poate considera submulțimea lui N, $xR = \{y \in N \mid xRy\}$. În cazul cînd $xR \neq \emptyset$, se spune că ρ (sau R) este definită în x. *Domeniul de definiție* al unei relații $R : M \to N$ este mulțimea D_R a tuturor elementelor din M în care R este definită; așadar,

$$D_R = \{x \in M \mid \exists\, y \in N \text{ astfel încît } xRy\}.$$

Codomeniul relației $R : M \to N$ este mulțimea

$$C_R = \{y \in N \mid \exists\, x \in M \text{ astfel încît } xRy\} = \bigcup_{x \in D_R} xR.$$

O imagine sugestivă este dată în fig. 1.3, unde D_R și C_R se obțin prin „proiecția" lui R pe mulțimile M și N.

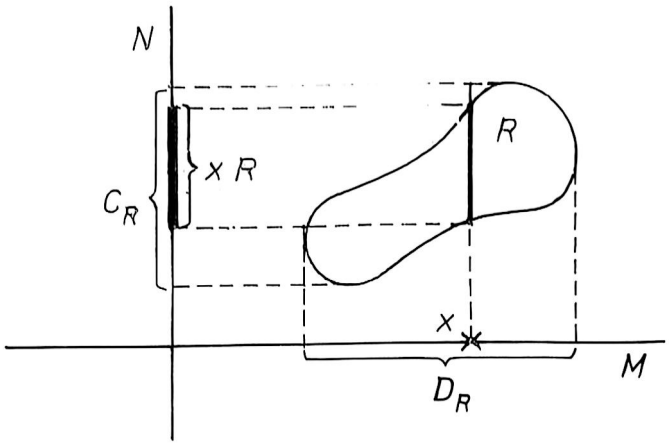


Fig. 1.3

Reluînd un exemplu dat anterior (lucrări-descriptori), se observă că domeniul relației R este M, iar codomeniul este format din acei descriptori din N care sînt efectiv utilizați pentru lucrările din acea bibliotecă.

Dacă $\rho : M \to N$, $\rho = (M, N, R)$ este o relație oarecare și $M' \subset M$, atunci se poate considera *restricția lui* ρ *la* M' ca fiind tripletul $\rho' = (M', N, R')$, unde $R' = R \cap (M' \times N)$; se mai notează $\rho' = \rho \mid M'$.

Uneori mulțimile M și N sînt subînțelese în funcție de context și atunci se vorbește simplu despre relația ρ (sau R) de la M la N. În cazul cînd $M = N$ se spune că avem o relație binară *pe* M. În cele ce urmează, vom nota cu $\mathrm{Rel}\, M$ mulțimea tuturor relațiilor binare pe M (deci a submulțimilor lui $M \times M$), adică

$$\mathrm{Rel}\, M = \mathbf{p}(M^2).$$

Exemple. 1) Fie $M = \{a, b\}$, $N = \{u, v\}$, $R = \{(a, u), (b, u), (a, v)\ (b, v)\}$, $S = \{(u, v), (v, u)\}$. Sînt astfel definite relațiile $\rho = (M, N, R)$ de la M la N și $\rho_1 \in \mathrm{Rel}\, N$, $\rho_1 = (N, N, S)$.

2) A defini o relație $\rho \in \mathrm{Rel}\, M$ revine la a fixa o colecție de perechi (x, y) de elemente din $M^2 = M \times M$. Să luăm $M = \mathbb{R}$ și $R = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$. Este definită astfel o relație $\rho = (M, M, R)$ pe mulțimea $\mathbb{R}$, al cărei grafic este mulțimea R, identificată cu mulțimea punctelor circumferinței unitate din $\mathbb{R}^2$.

Compunerea relațiilor

Fie $\rho = (M, N, R)$ și $\rho_1 = (N, P, S)$ două relații astfel încît cosursa lui ρ coincide cu sursa lui ρ_1. În acest caz se poate defini *relația compusă*

$$\rho_1 \circ \rho = (M, P, T), \text{ unde } T = \{(m, p) \in M \times P \mid \exists\, n \in N, (m, n) \in R \text{ și } (n, p) \in S\}.$$

Graficul T al relației $\rho_1 \circ \rho$ se mai notează $S \circ R$.

Pentru orice relație $\rho = (M, N, R)$ se definește *relația inversă*

$$\rho^{-1} = (N, M, R^{-1}), \text{ unde } R^{-1} \quad \{(n, m) \in N \times M \mid mRn\}.$$

Evident, $\rho \circ \rho^{-1} = (N, N, U_1)$ și $\rho^{-1} \circ \rho = (M, M, U_2)$, unde

$$U_1 = \{(n, n') \in N \times N \mid \exists\, m \in M, \quad mRn \text{ și } mRn'\};$$

$$U_2 = \{(m, m') \in M \times M \mid \exists\, n \in N, \quad mRn \text{ și } m'Rn\}.$$

Tipuri particulare de relații

Fie o relație (M, N, R) sau, cu notație echivalentă, $R : M \to N$. Ea se numește:

injectivă, dacă xRy și $x'Ry \Rightarrow x = x'$;
surjectivă, dacă $\forall\, y \in N, \exists\, x \in M$ astfel încît xRy;
totală, dacă $\forall\, x \in M, \exists\, y \in N$ astfel încît xRy (adică $D_R = M$);
funcțională, dacă xRy și $xRy' \Rightarrow y = y'$.

Relația $R : M \to N$ se numește *bijectivă* (*bijecție* sau, echivalent, *corespondență bijectivă*) între mulțimile M și N, dacă este totală, funcțională, injectivă și surjectivă. Nu între orice două mulțimi poate exista o corespondență bijectivă.

Funcții parțiale, funcții totale

Noțiunea de funcție este esențială în orice descrieri deoarece ea exprimă relații de asociere între elementele diverselor mulțimi.

Una din ideile principale ale oricărei modelări și programări matematice este aceea de a asocia numere, seturi de numere sau alte obiecte-standard unor entități eventual extramatematice; ingredientul principal al oricărei realizări a acestei idei îl constituie funcțiile. De exemplu, datele de ieșire la un calculator sînt funcție de datele de intrare, iar într-un compilator setul de instrucțiuni în limbaj-mașină

este funcție de programul impus. În aceste exemple apar în mod firesc funcțiile parțiale.

Dacă M și N sînt două mulțimi, se numește *funcție parțială de la M la N* orice relație funcțională (M, N, f), adică $f \subset M \times N$ astfel încît de îndată ce $x \in M$, $y, y' \in N$ și xfy, xfy', rezultă $y = y'$.

În acest caz este definită o funcție în sens uzual:

$$D_f \to N,\ x \mapsto \text{acel unic } y \in N \text{ astfel încît } xfy.$$

Se mai scrie atunci $y = f(x)$ pentru orice $x \in D_f$. Graficul lui f este $G_f = \{(x, f(x)) \mid x \in D_f\} \subset M \times N$. Dacă $D_f = M$, se spune că $f : M \to N$, $x \mapsto f(x)$ este *peste tot definită* sau că este o *funcție totală* de la M la N. Vom nota cu N^M mulțimea tuturor funcțiilor totale de la M la N. Dacă $f \in N^M$, atunci domeniul ei este $D_f = M$, iar codomeniul $C_f = \{f(x) \mid x \in M\}$. În cele ce urmează, printr-o funcție $f : M \to N$ vom înțelege o funcție totală numită ca de obicei și *aplicație* de la M la N. Dacă $A \subset M$, atunci se poate defini *restricția lui f la A*, $f|A : A \to N$, $x \mapsto f(x)$.

Dacă $f : M \to N$, $g : N \to P$ sînt două funcții (totale), atunci se poate considera relația compusă $g \circ f$ care este funcțională și se numește *funcția compusă*:

$$g \circ f : M \to P,\ x \mapsto g(f(x)).$$

Dacă M și N sînt două mulțimi de date (de exemplu, $M = N = \mathbb{R}$), atunci o funcție $f : M \to N$ asociază oricărei „date de intrare" $a \in M$, „rezultatul" $f(a)$, care aparține lui N. În acest context, compunerea de funcții este prezentată sugestiv în fig. 1.4.

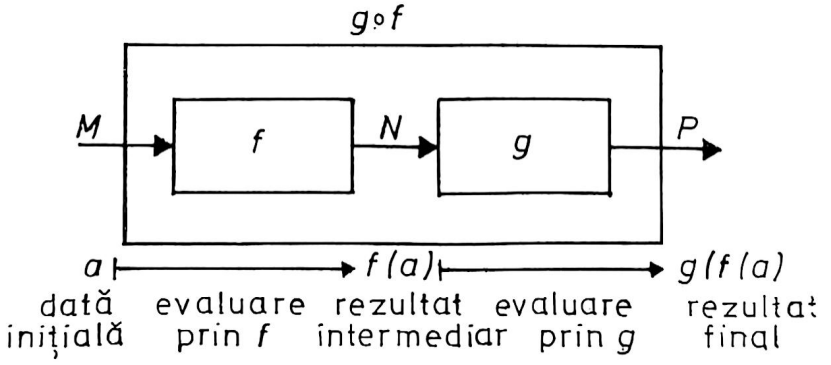


Fig. 1.4

Exemple. 1) Fie M o submulțime oarecare. Funcția identică $1_M : M \to M$, $x \mapsto x$ este bijectivă; graficul ei, $\Delta_M = \{(x, x) \mid x \in M\}$ este numit *diagonala* lui M.

Pentru orice aplicație $f : M \to N$, au loc relațiile $f \circ 1_M = f$ și $1_N \circ f = f$.

Există o unică relație de la $\emptyset$ la M, care este o funcție avînd graficul vid; dacă $M \neq \emptyset$, nu există nici o funcție $M \to \emptyset$.

2) Fie M_1, M_2 două mulțimi. Se pot considera aplicațiile surjective

$$p_1 : M_1 \times M_2 \to M_1,\ (a, b) \mapsto a;\ p_2 : M_1 \times M_2 \to M_2,\ (a, b) \mapsto b,$$

numite *proiecțiile canonice*. Pentru orice mulțime T și pentru orice aplicații $q_1 : T \to M_1$, $q_2 : T \to M_2$, există și este unică o aplicație $u : T \to M_1 \times M_2$ astfel încît $p_1 \circ u = q_1$, $p_2 \circ u = q_2$. Anume, $u(x) = (q_1(x), q_2(x))$, $\forall\, x \in T$. Aceasta se numește *proprietatea de universalitate a produsului cartezian* de mulțimi.

În mod similar se pot considera aplicațiile injective

$$i_1 : M_1 \to M_1 + M_2,\ x \mapsto (0, x);\ i_2 : M_2 \to M_1 + M_2,\ x \mapsto (1, x),$$

numite *injecțiile canonice*. Pentru orice mulțime T și pentru orice aplicații $j_1 : M_1 \to T$, $j_2 : M_2 \to T$, există și este unică o aplicație $v : M_1 + M_2 \to T$ astfel încît $v \circ i_1 = j_1$, $v \circ i_2 = j_2$ (*proprietatea de universalitate a sumei*). Anume, pentru orice $z \in M_1 + M_2$ rezultă două posibilități: sau $z \in \{0\} \times M_1$, $z = (0, x)$ și punem $v(z) = j_1(x)$ sau $z \in \{1\} \times M_2$, $z = (1, y)$ și atunci punem $v(z) = j_2(y)$.

3) În programare se consideră *funcția de adresare* $f : M \to N$, $a \mapsto a'$, care asociază oricărei adrese $a \in M$ conținutul a' al adresei respective. Dacă $M \cap N \neq \emptyset$ și $M_1 = \{a \in M \mid a \in M \cap N\}$, atunci se poate considera funcția $M_1 \to N$, $a \mapsto (a')' = a''$ etc.

Un rol deosebit în calculatoristică îl au funcțiile parțiale. Presupunem că se consideră un set de date S care ar putea fi introduse într-un program de calcul P. Atunci este în mod natural definită o funcție parțială $f_P : S \to T$ (T fiind mulțimea rezultatelor); funcția este parțială deoarece pentru anumite date $\alpha \in S$ programul poate să nu se oprească și valoarea $f_P(\alpha)$ nu este atunci definită.

O ultimă remarcă: modificînd codomeniul, orice funcție parțială $f : M \to N$ se transformă într-o funcție totală; anume, adjuncționăm la N un element $\perp \notin N$ și definim funcția $f^{\perp} : M \to N \cup \{\perp\}$, punînd

$$f^{\perp}(x) = \begin{cases} f(x) & \text{dacă } x \in D_f, \\ \perp & \text{dacă } f \text{ nu este definită în } x. \end{cases}$$

4) Fie I o mulțime fixată ale cărei elemente se numesc ad-hoc *indici*. Dacă E este o mulțime (din universul $\mathfrak{U}$), atunci prin *familie* de elemente din E se înțelege o aplicație $f : I \to E$; punînd $\forall\, i \in I$, $x_i = f(i)$, o astfel de familie se notează $\{x_i\}_{i \in I}$. Se numește familie de mulțimi $\{M_i\}_{i \in I}$ indexată după I, funcția $f : I \to \mathfrak{U}$, $i \mapsto M_i$. Se pot defini atunci:

— *reuniunea* acestei familii $\bigcup_{i \in I} M_i = \{x \mid \exists\, i \in I,\ x \in M_i\}$;

— *intersecția* $\bigcap_{i \in I} M_i = \{x \mid \forall\, i \in I,\ x \in M_i\}$;

— *produsul cartezian* $\prod_{i \in I} M_i = \{\{x_i\}_{i \in I} \mid \forall\, i \in I,\ x_i \in M_i\}$.

Dacă $I = \{1, 2\}$ se regăsesc $M_1 \cup M_2$, $M_1 \cap M_2$, $M_1 \times M_2$. Dacă $I = \mathbb{N}$ termenul de familie este înlocuit prin cel de *șir*.

5) Operațiile algebrice (numite și legi de compoziție) și predicatele (condițiile) sînt cazuri particulare de funcții.

Dacă M este o mulțime, reamintim că o *operație algebrică* (binară) pe M este o funcție parțială $* : M \times M \to M$. Dacă $*$ este totală, se spune că operația este peste tot definită și în acest caz, oricărei perechi $(x, y) \in M \times M$ i se asociază un element bine definit din M, notat $*(x, y)$ sau, echivalent, $x * y$.

Predicate

Prin *predicat unar* pe M se înțelege o funcție totală $\mathbf{p} : M \to \mathbb{B} = \{\mathbf{F}, \mathbf{A}\}$; mulțimea $M_\mathbf{p} = \{x \in M \mid \mathbf{p}(x) = \mathbf{A}\}$ se numește *mulțimea de adevăr* a lui $\mathbf{p}$. Dacă $x \in M_\mathbf{p}$, adică $\mathbf{p}(x) = \mathbf{A}$, se mai spune că $\mathbf{p}$ *este adevărat* pe elementul x (sau că x *satisface condiția* $\mathbf{p}$) și se scrie simplu $\mathbf{p}x$. Predicatele pe M modelează proprietăți (sau condiții) relativ la elementele lui M.

Un *predicat binar* este o funcție totală $M^2 \to \mathbb{B}$; aceasta permite descrierea valabilității unor proprietăți relativ la perechi de elemente din M.

Ca un exemplu concret fie M $\mathbb{Z}$. Pentru orice număr întreg $x \in \mathbb{Z}$ punem

$$\mathbf{p}(x) = \begin{cases} \mathbf{A} & \text{dacă } x \text{ este un număr prim,} \\ \mathbf{F} & \text{în caz contrar.} \end{cases}$$

Este astfel definit un predicat unar, $\mathbf{p} : \mathbb{Z} \to \mathbb{B}$, având ca mulțime de adevăr mulțimea numerelor prime. Așadar, $x \in \mathbb{Z}$ este prim $\leftrightarrow \mathbf{p}(x) = \mathbf{A}$. În mod similar, condiția $x \leqslant y$ este strîns legată de predicatul binar $q : \mathbb{Z}^2 \to \mathbb{B}$, definit prin

$$q(x, y) = \begin{cases} \mathbf{A} & \text{dacă } x \leqslant y, \\ \mathbf{F} & \text{în caz contrar.} \end{cases}$$

Relații de ordine și relații de echivalență

DEFINIȚIA 1.2. Fie M o mulțime și $R \in \operatorname{Rel} M$ o relație binară pe M. Relația R se numește:

— *reflexivă*, dacă $\forall\, x \in M$, xRx;

— *simetrică*, dacă $\forall\, x, y \in M$, $xRy \Rightarrow yRx$ (adică $R = R^{-1}$);

— *antisimetrică*, dacă $\forall\, x, y \in M (xRy$ și $yRx) \Rightarrow x = y$ (adică $R \cap R^{-1} \subset 1_M$);

— *tranzitivă*, dacă $\forall\, x, y, z \in M$, $(xRy$ și $yRz) \Rightarrow xRz$ (adică $R \circ R \subset R$).

O relație reflexivă și simetrică se numește *relație de compatibilitate*.

Se numește *preordine* o relație reflexivă și tranzitivă.

O preordine antisimetrică se numește *relație de ordine parțială*; dacă, în plus, $\forall\, x, y \in M$ avem (xRy) sau (yRx), atunci ordinea se numește *liniară*. Prin *relație de echivalență* se înțelege o preordine simetrică.

Exemple. 1) Dacă a este o mulțime având cel puțin două elemente, atunci relația de incluziune pe mulțimea $\mathfrak{p}(a)$ a părților lui a definește o relație de ordine parțială care nu este liniară.

2) Două mulțimi M și N din universul $\mathfrak{U}$ se numesc *echipotente* și se scrie $M \sim N$, dacă există o corespondență bijectivă de la M la N. Relația de echipotență pe $\mathfrak{U}$ este o relație de echivalență.

DEFINIȚIA 1.3. O mulțime pe care este fixată o relație de ordine parțială se numește *mulțime ordonată.*

Fie $(M, \leqslant)$ o mulțime nevidă ordonată (așadar, „$\leqslant$" este o relație reflexivă, tranzitivă și antisimetrică pe M). Fie $X \subset M$ o parte nevidă fixată. Un element $a \in M$ este numit:

— *cel mai mic element al lui* X, dacă $a \in X$ și $\forall\, x \in X$, $a \leqslant x$ (dacă există, acesta este unic și se notează $\min X$);

— un *element minimal* al lui X, dacă $a \in X$ și, în plus, $\forall\, x \in X$ nu avem $x < a$ (reamintim că $u < v$ înseamnă $u \leqslant v$ și $u \neq v$). X poate avea mai multe elemente minimale sau nici unul;

— *minorant* al lui X, dacă $\forall\, x \in X$, $a \leqslant x$; dacă mulțimea X admite cel puțin un minorant, atunci ea se numește *minorată* (sau *mărginită inferior*);

— *marginea inferioară* a lui X, dacă X are minoranți și a este cel mai mic minorant (se notează atunci $a = \inf X$ sau $a = \prod X$). Dacă a este cel mai mic element al lui X, atunci el este minimal și în plus $\prod X = a$.

În mod similar (dual) se definesc *cel mai mare element, elementele maximale, majoranții și marginea superioară* pentru o parte $X \subset M$ a unei mulțimi ordonate. Dacă există, marginea superioară a lui X se notează $\sup X$ sau $\bigsqcup X$.

Orice parte nevidă și liniar ordonată $L \subset M$ se mai numește *lanț*; așadar, $L \neq \emptyset$ și pentru orice $x, y \in L$ avem fie $x \leqslant y$, fie $y \leqslant x$.

DEFINIȚIA 1.4. Fie $(M, \leqslant)$ și $(N, \subseteq)$ două mulțimi ordonate. O aplicație $f : M \to N$ se numește *izotonă* (sau *monoton crescătoare*), dacă

$$\forall\, u, v \in M,\ u \leqslant v \Rightarrow f(u) \subseteq f(v).$$

Se mai spune că aplicațiile izotone păstrează ordinea.

Exemple. 1) Mulțimea $\mathbb{Z}$ este liniar ordonată relativ la ordinea uzuală $\leqslant$; în plus, orice parte nevidă a lui $\mathbb{Z}$ este un lanț.

2) Fie E o mulțime; atunci mulțimea $M = \mathfrak{p}(E)$ este ordonată relativ la incluziune ($\subset$); cel mai mic element este $\emptyset$, iar cel mai mare element este E. Dacă $X \subset M$, atunci X este o colecție de părți ale lui E; în acest caz, $\prod X$ (resp. $\bigsqcup X$) este tocmai intersecția (resp. reuniunea) mulțimilor din această colecție.

3) Dacă $f : M \to N$ este o aplicație izotonă și $L \subset M$ este un lanț, atunci $f(L) = \{f(x) \mid x \in L\}$ este un lanț; într-adevăr, $\forall\, u, v \in f(L)$, $\exists\, x, y \in L$ astfel ca $u = f(x)$,

$v = f(y)$. Deoarece L este un lanț, avem $x \leqslant y$ și atunci $u \leqslant v$ sau $y \leqslant x$ și atunci $v \leqslant u$. Prin urmare $f(L)$ este un lanț.

Fie acum $\rho' = ,,\equiv''$ o relație de echivalență pe o mulțime nevidă M. Pentru orice $x \in M$ se poate considera clasa de echivalență a lui x, anume $[x] = \{y \in M \mid y \equiv x\}$, notată uneori $\hat{x}$. Pentru orice $x, y \in M$ avem $x \in [x]$ și

$$(x \equiv y) \leftrightarrow [x] = [y].$$

Mulțimea tuturor claselor $[x]$, $x \in M$, se notează M/ρ și se numește *mulțimea-cît* a lui M prin relația $\rho = ,,\equiv''$. Două clase sînt distincte, dacă și numai dacă ele sînt disjuncte. Dacă din fiecare clasă se „extrage" cîte un element, atunci este definit un sistem complet de reprezentanți S; familia $\{[x]\}_{x \in S}$ de părți ale lui M constituie evident o partiție a mulțimii M.

Ideea fundamentală în considerarea mulțimii-cît este aceea de a înlocui relația de echivalență $\rho = ,,\equiv''$ pe M prin relația de egalitate $,,=''$ pe mulțimea M/ρ. Multe construcții matematice (construcția lui $\mathbb{Z}$ și $\mathbb{Q}$ pornind de la $\mathbb{N}$, construcția lui Cantor a lui $\mathbb{R}$, vectorii liberi, cardinalele de mulțimi, completarea unui spațiu metric, integrala Lebesgue, automatele reduse etc.) folosesc această idee, una din dificultăți fiind asimilarea și actualizarea claselor de echivalență ca noi entități matematice.

Exemplu. Fie $,,\leqslant''$ o relație de preordine pe o mulțime nevidă M; pentru $x, y \in M$ se pune

$$x \sim y \leftrightarrow (x \leqslant y \text{ și } y \leqslant x).$$

În acest caz se obține o relație de echivalență pe M și, în plus, mulțimea-cît $M/\sim$ este o mulțime ordonată, definind $\forall\, x, y \in M$,

$$[x] \leqslant [y] \leftrightarrow x \leqslant y.$$

Interpretarea sistemică a relațiilor

Fie $\rho = (M, N, R)$ o relație binară de la mulțimea M la mulțimea N. Vom numi *ad-hoc* elementele lui M *intrări*, iar elementele lui N *ieșiri*, deci R este o colecție de perechi intrare-ieșire. Dacă $x \in M$, $y \in N$ și dacă xRy, atunci se mai scrie: $x \xrightarrow{R} y$ și se spune că ieșirea y este „declanșată" de intrarea x. Pentru orice $x \in M$, $xR = \{y \in N \mid xRy\}$ este mulțimea ieșirilor declanșate de x și pentru orice $y \in N$, $Ry = \{x \in M \mid xRy\}$ este mulțimea intrărilor care declanșează ieșirea y. Relația R este definită în x dacă $xR \neq \emptyset$, adică x declanșează efectiv ieșiri.

Aşadar, o relaţie ρ se poate asimila cu un *sistem intrare-ieşire* (v. fig. 1.5).

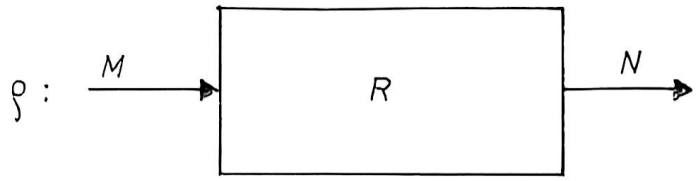


Fig. 1.5

Dacă relaţia ρ este funcţională totală, atunci sistemul intrare-ieşire asociat este deterministic, în sensul că oricărei intrări $x \in M$ îi corespunde o ieşire bine determinată $y = R(x) \in N$.

Fie $\rho = (M, N, R)$ şi $\rho_1 = (N, P, S)$ două sisteme intrare-ieşire în care mulţimea ieşirilor primului sistem coincide cu mulţimea intrărilor celui de al doilea. Atunci sistemul

$$\rho_1 \circ \rho = (M, P, T), \quad T = S \circ R,$$

obţinut prin compunerea relaţiilor ρ, ρ_1 în această ordine, se numeşte *cuplajul în serie* al sistemelor considerate. Aşadar, o intrare $x \in M$ declanşează o ieşire $y \in P$ (în $\rho_1 \circ \rho$), dacă şi numai dacă există $u \in N$ astfel încît $x \xrightarrow{R} u$ şi $u \xrightarrow{S} y$ (v. fig. 1.6.).

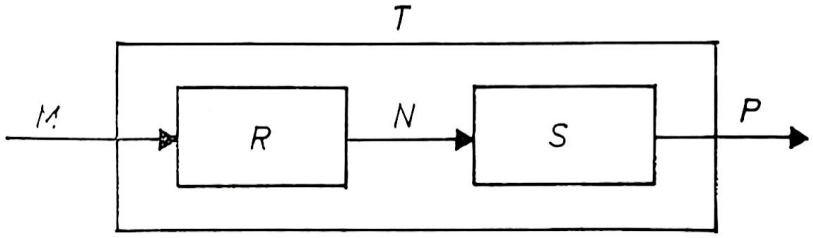


Fig. 1.6

Dacă $\rho_1 = (M_1, N_1, R_1)$, $\rho_2 = (M_2, N_2, R_2)$ sînt două sisteme intrare-ieşire oarecare, atunci se poate defini *cuplajul lor în paralel* (v. fig. 1.7).

$$\rho_1 \times \rho_2 = (M_1 \times M_2, N_1 \times N_2, R_1 \times R_2).$$

Aşadar, o intrare $(x_1, x_2) \in M_1 \times M_2$ declanşează o ieşire $(y_1, y_2) \in N_1 \times N_2$ (în $\rho_1 \times \rho_2$), dacă şi numai dacă $x_1 \xrightarrow{R_1} y_1$ şi $x_2 \xrightarrow{R_2} y_2$.

Dacă $M_1 = M_2 = M$, atunci se poate considera de asemenea $(M_1, N_1 \times N_2, R)$, o intrare $x \in M$ declanşînd o ieşire $(y_1, y_2) \in N_1 \times N_2$, dacă şi numai dacă $x \xrightarrow{R_1} y_1$ şi $x \xrightarrow{R_2} y_2$ (v. fig. 1.8).

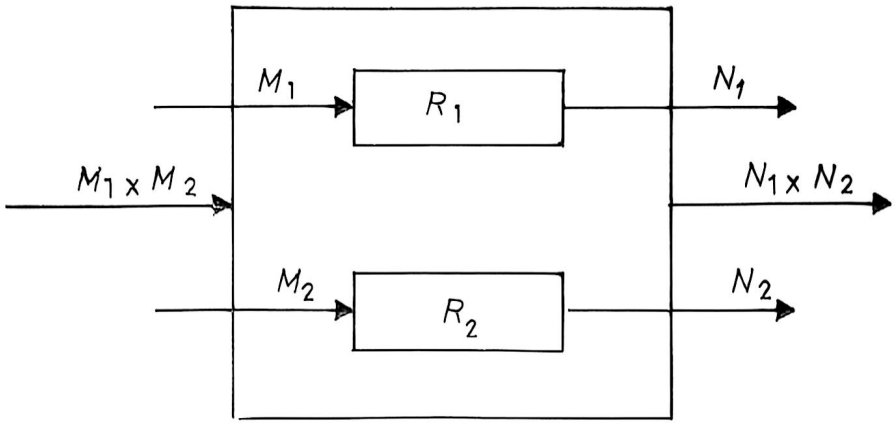


Fig. 1.7

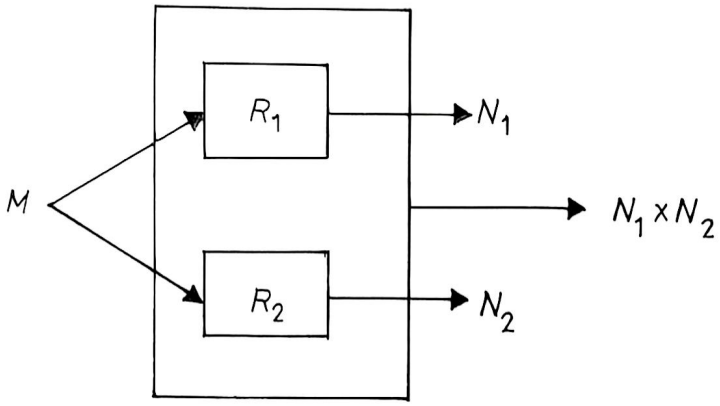


Fig. 1.8

Dacă relaţiile considerate mai sus sînt relaţii funcţionale totale, atunci aceeaşi proprietate o au cuplările lor (în serie, în paralel etc.).

§ 1.2. DINAMICI PEANO

Cea mai importantă clasă de numere este mulţimea $\mathbb{N}$ a numerelor naturale. O întrebare mereu actuală este următoarea : ce entităţi matematice pot fi construite pornind de la $\mathbb{N}$? O dată cu construcţia, axiomatică, datorată lui G. Peano (1858-1932), a mulţimii $\mathbb{N}$ s-a declanşat un nou pitagoreism, prin considerarea numărului ca obiect primar de reflexie ; aceasta a condus, printre altele, la elaborarea conceptului de funcţie recursivă şi implicit la caracterizarea funcţiilor ale căror valori pot fi calculate prin mijloace mecanizabile, unul din succesele majore ale matematicii discrete, obţinut în ultimii ani.

În esenţă, orice calcul angajează două entităţi : date iniţiale şi o dinamică de prelucrare a lor. Mulţimea $\mathbb{N}$ este cel mai simplu exemplu unde se ilustrează acest fapt (0 = zero ca dată iniţială şi funcţia-succesor ca dinamică).

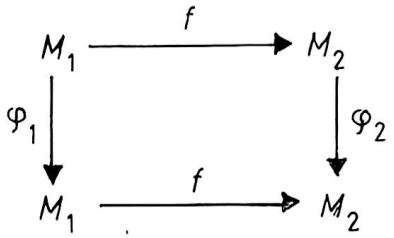
Dinamici

DEFINIȚIA 1.5. Vom numi *dinamică* orice pereche (M, φ) alcătuită dintr-o mulțime M și o aplicație $\varphi : M \to M$.

Dacă (M_1, φ_1) și (M_2, φ_2) sînt două dinamici, prin *morfism de dinamici* (sau *dinamorfism*)

$$(M_1, \varphi_1) \to (M_2, \varphi_2)$$

vom înțelege o aplicație $f : M_1 \to M_2$ astfel încît $\forall\, a \in M_1, f(\varphi_1(a)) = \varphi_2(f(a))$, adică diagrama



să fie comutativă. Dacă în plus f este bijectivă se mai spune că dinamicile (M_1, φ_1), (M_2, φ_2) sînt *izomorfe*.

Noțiunea de dinamică este datorată în esență lui R. Dedekind (1831-1916) ([5]).

Dacă (M, φ) este o dinamică, atunci funcția identică 1_M definește evident un dinamorfism $(M, \varphi) \to (M, \varphi)$ numit *morfismul identic* al dinamicii. Dacă (M_1, φ_1), (M_2, φ_2) și (M_3, φ_3) sînt dinamici și $M_1 \xrightarrow{f} M_2$, $M_2 \xrightarrow{g} M_3$ sînt dinamorfisme, atunci $g \circ f$ este un dinamorfism $(M_1, \varphi_1) \to (M_3, \varphi_3)$.

Vom vedea că dinamicile și dinamorfismele formează o categorie.

O subdinamică a unei dinamici (M, φ) este o parte $S \subset M$ astfel încît $\varphi(S) \subset S$, adică $\forall\, x \in S$, $\varphi(x) \in S$. În acest caz, $(S, \varphi|S)$ este și ea o dinamică. Este evident că intersecția unei familii oarecare de subdinamici este o subdinamică; de asemenea, reuniunea unei familii oarecare de subdinamici este o subdinamică.

Dacă (M, φ) este o dinamică, atunci pentru orice $A \subset M$ se poate defini subdinamica

$$\bar{A} = \bigcap \{S | S \text{ este subdinamică a lui } (M, \varphi) \text{ și } A \subset S\},$$

numită *subdinamica lui* (M, φ) *generată de* A. Pentru $a \in M$ vom scrie $\bar{a}$ în loc de $\{\bar{a}\}$; desigur, $\bar{a}$ este cea mai mică subdinamică a lui (M, φ) care conține elementul a.

Dinamici cu inițializare

Vom spune că o dinamică (M, φ) *are inițializare* dacă este fixat un element $a \in M$; ea se va nota atunci $(M, \varphi)_a$. Un *morfism de dinamici cu inițializare* $(M, \varphi)_a \to (M', \varphi')_{a'}$ este o funcție $f : M \to M'$, astfel încît $\varphi' \circ f = f \circ \varphi$ și $f(a) = a'$. Se definesc în mod natural compunerea a două astfel de morfisme și morfismul identic al unei dinamici cu inițializare.

DEFINIȚIA 1.6 ([25]). Prin *dinamică Peano* vom înțelege o dinamică având inițializare $(N, s)_0$, deci o aplicație $s : N \to N$ și un element $0 \in N$, astfel încît să fie verificate următoarele trei condiții:

P1. Pentru orice $n \in N$, $s(n) \neq 0$ (adică $0 \notin s(N)$);

P2. Aplicația s este injectivă;

P3. Dacă $A \subset N$, $0 \in A$ și $s(A) \subset A$, atunci $A = N$.

Pentru orice $a \in N$ elementul $s(a)$ se numește *succesorul lui* a. Condiția P3 evidențiază faptul că orice subdinamică a lui (N, s) care conține 0, coincide cu N și poate fi formulată pe scurt astfel: $\overline{0} = N$.

Un exemplu tipic de dinamică Peano îl constituie desigur tripletul $(\mathbb{N}, s)_0$ format din mulțimea numerelor naturale (presupusă construită), funcția-succesor uzuală $s : \mathbb{N} \to \mathbb{N}$, $n \mapsto n + 1$ și inițializarea $0 \in \mathbb{N}$. În cele ce urmează, nu vom presupune construită apriori mulțimea $\mathbb{N}$, ci vom ajunge la ea tocmai VIA conceptul de dinamică Peano.

LEMA 1. *Să considerăm o dinamică Peano* $(N, s)_0$. *Atunci* $s(N) = N \setminus \{0\}$ *și, în plus,* $\forall\, n \in N$, $n \neq s(n)$.

Demonstrație. Fie $A = s(N) \cup \{0\}$. Deoarece $A \subset N$, $0 \in A$ și $s(A) \subset A$, rezultă conform P3 că $A = N$, adică $N = s(N) \cup \{0\}$. Conform P1, $0 \notin s(N)$, deci $s(N) = N \setminus \{0\}$.

Să presupunem apoi că ar exista $n \in N$ astfel încît $n = s(n)$. Atunci $n \neq 0$ și considerînd mulțimea $B = N \setminus \{n\}$, rezultă $0 \in B$. Pentru orice $m \in B$ avem $m \neq n$ și prin urmare $s(m) \neq s(n)$, conform P2. Ca atare $s(m) \neq n$, deci $s(m) \in B$. Conform P3 rezultă $B = N$, ceea ce este absurd. ∎

LEMA 2 (*principiul I al inducției matematice*). *Fie* $(N, s)_0$ *o dinamică Peano și* $\pi : N \to \mathbb{B} = \{\mathbf{F}, \mathbf{A}\}$ *un predicat unar pe* N, *astfel încît* $\pi 0$ (*adică* $\pi(0) = \mathbf{A}$) *și* $\{\forall\, k \in N, \pi k \Rightarrow \pi s(k)\}$. *Atunci,* $\forall\, n \in N$, πn (*adică* $\pi(n) = \mathbf{A}$).

Demonstrație. Fie $C = M_\pi$, mulțimea de adevăr a predicatului π. Conform ipotezei rezultă că $0 \in C$ și că $\forall\, k \in C \Rightarrow s(k) \in C$, adică $s(C) \subset C$. Conform P3 rezultă $C = N$, adică predicatul π este adevărat pe orice element $n \in N$. ∎

Desigur lema 2 modelează faptul că dacă o anumită proprietate π relativ la elementele lui N are loc pentru 0 (baza inducției) și dacă are loc implicația $\pi(k) \Rightarrow \pi(s(k))$ (pasul inducției), atunci proprietatea π are loc pentru toate elementele lui N. Vom vedea mai tîrziu că lema 2 se extinde la cazul cînd baza inducției este un element $n_0 \in N$.

Caracterizarea dinamicilor Peano

Vom da acum o teoremă care fundamentează definirea prin recurență a unor obiecte matematice care depind de un număr natural, după schema următoare:

— se definește obiectul care corespunde lui 0;

— se definește obiectul care corespunde lui $s(n)$ cu ajutorul obiectului deja definit pentru n.

Existența acestor obiecte nu este asigurată de principiul inducției matematice; acest principiu este utilizat cel mult pentru a demonstra proprietăți ale acestor obiecte, după ce acestea au fost definite. Așa cum vom vedea, definirea prin recurență presupune organizarea ca dinamică a domeniului de unde sînt selectate obiectele.

TEOREMA 1.1 (*proprietatea de inițialitate a dinamicilor Peano*) ([25]). *Fie* $(N, s)_0$ *o dinamică Peano. Oricare ar fi dinamica avînd inițializare* $(M, \varphi)_a$, *există și este unic un morfism de dinamici cu inițializare* $f : N \to M$ *astfel încît* $f(0) = a$.

Demonstrație. În cazul cînd N ar fi mulțimea numerelor naturale cu structura Peano uzuală (adică $s : N \to N$, $n \mapsto n + 1$ și 0 este cel mai mic număr natural), construcția lui f este manifestă: $\forall\, n \in N$, $f(n) = \varphi^n(a)$, unde $\varphi^n = \varphi \overset{n \text{ ori}}{\circ \ldots \circ} \varphi$. Dar în cazul general și în condițiile cînd nu presupunem construită (în acest moment) mulțimea numerelor naturale, demonstrația este ceva mai subtilă și este prezentată în continuare.

Fie $\mathfrak{R}$ mulțimea relațiilor binare ρ de la N la M astfel încît $0 \rho a$ și de îndată ce $n \rho m$ să rezulte $s(n) \rho \varphi(m)$. Mulțimea $\mathfrak{R}$ este nevidă deoarece conține relația banală $(N, M, N \times M)$ și fie $f = \bigcap_{\rho \in \mathfrak{R}} \rho$. Este evident că $f \in \mathfrak{R}$.

Ne propunem să arătăm că *relația* $f : N \to M$ *este o funcție totală*. Mai întîi arătăm că $\forall\, n \in N$, $\exists\, m \in M$ astfel încît $(n, m) \in f$. Pentru aceasta, aplicăm inducția după n, mai precis lema 2: avem $(0, a) \in f$ și de îndată ce există $m \in M$ astfel încît $(n, m) \in f$ rezultă că există $\varphi(m) \in M$ și $(s(n), \varphi(m)) \in f$. Așadar, relația f este totală.

Rămîne să arătăm că f este relaţie funcţională : presupunem că $n, m_1, m_2 \in M$ şi $(n, m_1) \in f$, $(n, m_2) \in f$; avem de arătat că $m_1 = m_2$; pentru aceasta folosim din nou inducţia după n. Dacă $n = 0$ rezultă că $(0, m_1) \in f$ şi $(0, m_2) \in f$. Vom arăta că $m_1 = a$ şi similar se va arăta că $m_2 = a$, deci $m_1 = m_2$. Dacă, prin absurd, $m_1 \neq a$, atunci relaţia $g = f \setminus \{(0, m_1)\}$ aparţine lui $\mathcal{R}$ [ea conţine deci $(0, a)$ şi, în plus, dacă $(n, m) \in g$, atunci $(n, m) \in f$ şi cum $f \in \mathcal{R}$, $(s(n), \varphi(m)) \in f$; apoi, aplicînd lema 1 avem $(s(n), \varphi(m)) \neq (0, m_1)$, deci $(s(n), \varphi(m)) \in g$]. Deoarece g este o relaţie din $\mathcal{R}$, rezultă că $f \subset g$ (deoarece $f = \bigcap_{\rho \in \mathcal{R}} \rho$) şi se ajunge la o contradicţie. Afirmaţia este demonstrată pentru $n = 0$. Realizăm acum pasul de inducţie : presupunem deci că elementul $n \in N$ are proprietatea că ori de cîte ori $m_1', m_2' \in M$ şi $(n, m_1') \in f$, $(n, m_2') \in f$, rezultă $m_1' = m_2'$ şi demonstrăm că o proprietate similară o are $s(n)$. Admitem că $m_1, m_2 \in M$ şi $(s(n), m_1) \in f$, $(s(n), m_2) \in f$ şi avem de arătat că $m_1 = m_2$. Relaţia f fiind totală, există $m \in M$ astfel ca $(n, m) \in f$ şi vom proba că $m_1 = \varphi(m)$ [în mod similar se va arăta că $m_2 = \varphi(m)$, de unde rezultă $m_1 = m_2$]. Dacă, prin absurd, am avea $m_1 \neq \varphi(m)$, atunci să considerăm relaţia $h = f \setminus \{(s(n), m_1)\}$. Vom arăta că $h \in \mathcal{R}$, deci o contradicţie. Avem $(0, a) \in h$, deoarece $(0, a) \in f$ şi $0 \neq s(n)$. Fie apoi $(n', m') \in h$, deci $(n', m') \in f$ şi $(n', m') \neq (s(n), m_1)$. Deoarece $(n', m') \in f$, rezultă $(s(n'), \varphi(m')) \in f$ şi avem de arătat că $(s(n'), \varphi(m')) \neq (s(n), m_1)$, de unde se deduce că $(s(n'), \varphi(m')) \in h$ şi ca atare că $h \in \mathcal{R}$. Or, dacă $(s(n'), \varphi(m')) = (s(n), m_1)$, atunci rezultă $\varphi(m') = m_1$ şi $s(n) = s(n')$, deci $n = n'$ (s fiind injectivă); elementele $(n', m') = (n, m')$ şi (n, m) aparţin lui f şi, conform ipotezei de inducţie, rezultă $m = m'$, de unde $\varphi(m) = \varphi(m') = m_1$, ceea ce contravine ipotezei că $m_1 \neq \varphi(m)$.

Am demonstrat deci existenţa unei funcţii (totale) $f : N \to M$ astfel încît $f(0) = a$, cu proprietatea că de îndată ce $f(n) = m$, rezultă $f(s(n)) = \varphi(m)$, adică $f \circ s = \varphi \circ f$, deci f este un morfism de dinamici cu iniţializare.

Rămîne să arătăm unicitatea lui f. Dacă $f' : N \to M$ este un alt morfism de dinamici cu iniţializare astfel încît $f'(0) = a$, atunci $f' \circ s = \varphi \circ f'$. Se demonstrează imediat, prin inducţie, că $\forall\, n \in N$, $f(n) = f'(n)$; într-adevăr, avem $f(0) = f'(0) = a$ şi dacă această afirmaţie are loc pentru n, atunci $f(s(n)) = \varphi(f(n)) = \varphi(f'(n)) = f'(s(n))$, deci afirmaţia are loc şi pentru $s(n)$.

Observaţie. Teorema 1.1 admite o reciprocă : *dacă $(N, s)_0$ este o dinamică cu iniţializare, astfel încît pentru orice dinamică cu iniţializare $(M, \varphi)_a$ să existe şi să fie unic un morfism de dinamici $f : N \to M$ cu $f(0) = a$, atunci $(N, s)_0$ este o dinamică Peano.* Pentru demonstraţie trebuie verificate condiţiile P1, P2, P3 din definiţia 1.6.

Pentru a verifica P1, să considerăm dinamica $(\mathbb{B}, \delta)$, unde $\mathbb{B} = \{\mathbf{F}, \mathbf{A}\}$ şi $\delta : \mathbb{B} \to \mathbb{B}$, $x \mapsto \mathbf{A}$, cu iniţializarea $a = \mathbf{F}$. Conform ipotezei, există un morfism de dinamici $h : N \to \mathbb{B}$

astfel încît $h(0) = \mathbf{F}$. Dacă ar exista $n \in \mathbb{N}$, astfel încît $s(n) = 0$, atunci ar rezulta că $\mathbf{A} = \delta(h(n)) = h(s(n)) = h(0) = \mathbf{F}$, ceea ce este absurd. Verificăm apoi P2 și pentru aceasta, adjuncționăm la mulțimea N un element $\perp \notin N$. Considerăm astfel mulțimea $N' = N \cup \{\perp\}$ și aplicația $s' : N' \to N'$,

$$s'(n) = \begin{cases} s(n) & \text{dacă } n \in N, \\ 0 & \text{dacă } n = \perp. \end{cases}$$

Aplicația de incluziune $j : N \to N'$, $n \mapsto n$ este un morfism de dinamici cu inițializare de la $(N, s)_0$ la $(N', s')_0$, deoarece $\forall\, n \in N$, $j(s(n)) = s(n) = s'(n) = s'(j(n))$ și $j(0) = 0$. Conform ipotezei asupra lui $(N, s)_0$, există și este unic un morfism de dinamici $f : N \to N'$ astfel încît $f(0) = \perp$. Aplicația compusă $f \circ s : N \to N'$ este de asemenea un morfism de dinamici și, în plus, $(f \circ s)(0) = f(s(0)) = s'(f(0)) = s'(\perp) = 0$; morfismele j și $f \circ s$ îndeplinesc aceeași proprietate, deci ele coincid: $f \circ s = j$. De aici rezultă imediat că aplicația s este injectivă: dacă $s(n_1) = s(n_2)$, atunci $f(s(n_1)) = f(s(n_2))$, adică $j(n_1) = j(n_2)$, deci $n_1 = n_2$.

Rămîne să demonstrăm P3. Fie $A \subset N$, $0 \in A$ și $s(A) \subset A$. Atunci considerînd dinamica $(A, s|A)_0$, există un morfism de dinamici $f : N \to A$ astfel încît $f(0) = 0$. Notînd cu $i : A \to N$, $x \mapsto x$ aplicația de incluziune, rezultă că $i \circ f : N \to N$ este un morfism de dinamici și, în plus, $(i \circ f)(0) = i(f(0)) = i(0) = 0$. Așadar, morfismele de dinamici $i \circ f$ și 1_N coincid, deci $A = N$ (pentru orice $x \in \mathbb{N}$ avem $x = 1_N(x) = i(f(x)) = f(x) \in A$ și ca atare $N \subset A$).

Operațiile algebrice în N

Să fixăm o dinamică Peano $(N, s)_0$, adică un triplet $(N, s, 0)$ alcătuit dintr-o mulțime nevidă N, o aplicație $s : N \to N$ și un element $0 \in N$, verificînd condițiile P1, P2, P3. Notăm $1 = s(0)$. Vom indica în continuare modul cum se pot introduce operațiile algebrice de adunare și înmulțire în N folosind teorema 1.1. Astfel de considerații ar putea părea „tun pentru muște" dar ele au totuși o însemnătate principială, deoarece dinamicile Peano constituie cel mai simplu model de schemă recurențială cu inițializare, înzestrabilă cu o structură algebrică și cu o structură de ordine, reprezentînd totodată punctul de plecare al oricărui calcul.

Structura aditivă în N. Fie $m \in N$ un element arbitrar fixat. Conform teoremei 1.1 există și este unic un morfism de dinamici cu inițializare

$$f_m : (N, s)_0 \to (N, s)_m,$$

adică o funcție $f_m : N \to N$ astfel încît $f_m \circ s = s \circ f_m$ și $f(0) = m$. Pentru orice $m, n \in N$ se definește suma

$$m + n = f_m(n).$$

Dăm o listă de proprietăți ale *operației de adunare* astfel definite

$$+ : N \times N \to N, \quad (m, n) \mapsto m + n = f_m(n).$$

a) $\forall\, m, n \in N,\ m + 0 = m$ și $m + s(n) = s(m + n)$.
Într-adevăr, $f_m(0) = m$ și $f_m(s(n)) = s(f_m(n))$.

În particular, rezultă $m + s(0) = s(m)$, adică $m + 1 = s(m)$, pentru orice $m \in N$.

b) $\forall\, m \in N,\ m + 0 = 0 + m = m$.
Se aplică inducția după m (lema 2).

c) $\forall\, m, n, p \in N,\ m + (n + p) = (m + n) + p$.
Se aplică inducția după p.

d) $\forall\, m, n \in N,\ s(m + n) = s(m) + n$ și $m + n = n + m$.
Inducție după n.

e) Dacă $m, n, p \in N$ și $m + n \quad m + p$, atunci $n = p$.
Inducție după m, folosind faptul că aplicația s este injectivă.

f) Dacă $m, n \in N$ și $m + n = 0$, atunci $m = 0$ și $n = 0$.
Într-adevăr, dacă $n \neq 0$, atunci, conform lemei 1, ar rezulta că $n \in s(N)$, adică $n = s(p)$ cu $p \in N$. Deci $0 = m + n = f_m(n) = f_m(s(p)) = s(f_m(p))$, adică $0 \in s(N)$, ceea ce este absurd. Așadar, în mod necesar $n = 0$ și $m = 0$.

Structura multiplicativă în N. Fie $m \in N$ arbitrar fixat și dinamica având inițializare $(N, f_m)_0$. Conform teoremei 1.1 există și este unic un morfism de dinamici cu inițializare

$$g_m : (N, s)_0 \to (N, f_m)_0,$$

adică o funcție $g_m : N \to N$, astfel încît $g_m \circ s = f_m \circ g_m$ și $g_m(0) = 0$. Pentru orice $m, n \in N$ se definește *produsul*

$$m \cdot n = g_m(n).$$

Dăm o listă de proprietăți ale *operației de înmulțire*

$$\cdot : N \times N \to N,\ (m, n) \mapsto m \cdot n = g_m(n).$$

a) $\forall\, m, n \in N,\ m \cdot s(n) = m + m \cdot n$.
Aceasta reprezintă o transcriere a relației $g_m(s(n)) = f_m(g_m(n))$.

b) $\forall\, m \in N,\ m \cdot 0 = 0 \cdot m = 0$.
Faptul că $m \cdot 0 = 0$ rezultă din relația $g_m(0) = 0$, iar relația $0 \cdot m = 0$ se verifică prin inducție după m.

c) $\forall\, m, n, p \in N,\ m \cdot (n \cdot p) = (m \cdot n) \cdot p$.
Inducție după p.

d) $\forall\, m \in N,\ m \cdot 1 = 1 \cdot m = m$.

Mai întîi, $m \cdot 1 = m \cdot s(0) \overset{\text{cf. a)}}{=} m + m \cdot 0 \quad m$; relația $1 \cdot m = m$ se verifică prin inducție după m.

e) $\forall\, m, n \in \mathcal{N},\ m \cdot n = n \cdot m$.

Inducție după n, folosind d).

f) $\forall\, m, n, p \in \mathcal{N},\ m \cdot (n + p) = m \cdot n + m \cdot p$.

Folosim inducția după p. Pentru $p = 0$, relația rezultă din b). Presupunem afirmația adevărată pentru p; atunci $m \cdot (n + s(p)) = m \cdot [n + (p + 1)] = m \cdot [(n + 1) + p] = m \cdot (n + 1) + m \cdot p \overset{\text{cf. a)}}{=} (m \cdot n + m) + m \cdot p = m \cdot n + m \cdot (p + 1) = m \cdot n + m \cdot s(p)$, deci relația din enunț are loc pentru $s(p)$.

g) Dacă $m, n \in \mathcal{N}$ și $m \cdot n = 0$, atunci $m = 0$ sau $n = 0$.

Dacă, de exemplu, $m \neq 0$, atunci $m \in \mathcal{N} \setminus \{0\} = s(\mathcal{N})$ și ca atare există $m_1 \in \mathcal{N}$ astfel încît $m = s(m_1)$. Deci $0 = m \cdot n = s(m_1) \cdot n = m_1 \cdot n + n$ și folosind proprietatea f) a adunării rezultă $n = 0$.

Exponențierea. Fie $m \in \mathcal{N}$ arbitrar fixat și dinamica avînd inițializare $(\mathcal{N}, g_m)_1$. Conform teoremei 1.1, există și este unic un morfism de dinamici cu inițializare

$$h_m : (\mathcal{N}, s)_0 \to (\mathcal{N}, g_m)_1,$$

deci $h_m \circ s = g_m \circ h_m$ și $h_m(0) = 1$. Pentru orice $m, n \in \mathcal{N}$ se definește

$$m^n = h_m(n)$$

și *operația de exponențiere* $\mathcal{N} \times \mathcal{N} \to \mathcal{N}$, $(m, n) \mapsto m^n$.

Avem $h_m(s(n)) = g_m(h_m(n))$ și $h_m(0) = 1$, deci $m^{s(n)} = m \cdot m^n$ și $m^0 = 1$ pentru orice $m, n \in \mathcal{N}$.

Se verifică ușor că $\forall\, n \in \mathcal{N}, n \neq 0$, avem $0^n = 0$ și că $\forall\, m, n_1, n_2 \in \mathcal{N}$, $m^{n_1 + n_2} = m^{n_1} \cdot m^{n_2}$ etc.

Structura de ordine în N

Fixăm o dinamică Peano $(\mathcal{N}, s)_0$. Pentru orice $m, n \in \mathcal{N}$ definim

$$m \leqslant n \leftrightarrow \exists\, p \in \mathcal{N},\ m + p = n;\quad m < n \leftrightarrow m \leqslant n \text{ și } m \neq n.$$

Relațiile binare „$\leqslant$" și „$<$" astfel definite pe $\mathcal{N}$ au următoarele proprietăți care decurg din considerațiile anterioare:

a) „$\leqslant$" este o relație de ordine (adică este reflexivă, tranzitivă și antisimetrică).

Demonstrația este imediată.

b) $\forall\, n \in N,\ 0 \leqslant n$ și $n < s(n)$.

Într-adevăr, $0 + n = n$, deci $0 \leqslant n$. Apoi, $n + s(0) = s(n)$, deci $n \leqslant s(n)$, iar lema 1 arată că $n \neq s(n)$.

c) Aplicația $s : N \to N$ este izotonă: dacă $m, n \in N$ și $m \leqslant n$, atunci $s(m) \leqslant s(n)$.

Într-adevăr, dacă $m \leqslant n$, atunci $m + p = n$ cu $p \in N$ și $s(m) + p = s(m + p) = s(n)$, deci $s(m) \leqslant s(n)$.

d) Dacă $m, n \in N$ și $m < n$, atunci $s(m) \leqslant n$.

Fie $m + p = n$ cu $p \in N$. Deoarece $m \neq n$ rezultă $p \neq 0$, deci $p = s(p')$ cu $p' \in N$ și ca atare $s(m) + p' = n$.

e) Dacă $m, n \in N$ și $m \leqslant n \leqslant s(m)$, atunci $m = n$ sau $s(m) \quad n$.

Se folosește d).

f) Relația de ordine „$\leqslant$" pe N este liniară.

Avem deci de arătat că $\forall m, n \in N$, $m \leqslant n$ sau $n \leqslant m$. Pentru aceasta se fixează m și folosind d) se arată, prin inducție după n, că $\forall n$ avem $m \leqslant n$ sau $n \leqslant m$.

g) Dacă $m, n, p \in N$ și $n \leqslant p$, atunci $m + n \leqslant m + p$ și $m \cdot n \leqslant m \cdot p$.

Într-adevăr, conform ipotezei, există $q \in N$ astfel încît $n + q = p$, deci $(m + n) + q = m + (n + q) = m + p$ și $m + n \leqslant m + p$. Apoi, $m \cdot n + m \cdot q = m \cdot (n + q) = m \cdot p$ și $m \cdot n \leqslant m \cdot p$.

h) $\forall\, m, n, p \in N,\ m \neq 0,\ m \cdot n = m \cdot p \Rightarrow n = p$.

Conform lemei 1 avem $N \setminus \{0\} = s(N)$. Deoarece $m \neq 0$ rezultă atunci că există $m_1 \in N$ astfel încît $m = s(m_1)$. Conform f) avem $n \leqslant p$ sau $p \leqslant n$. În primul caz există $q \in N$ astfel încît $n + q = p$, deci $m \cdot n + m \cdot q = m \cdot p$; conform ipotezei se obține $m \cdot q = 0$, adică $s(m_1) \cdot q = 0$. Așadar, $0 = q + m_1 \cdot q$ și ca atare $q = 0$, deci $n = p$. Se procedează similar în cazul cînd $p \leqslant n$.

i) Fie $\mathbf{p} : N \to \mathbb{B} = \{\mathbf{F}, \mathbf{A}\}$ *un predicat (unar)* pe N și $n_0 \in N$ fixat. Dacă $\mathbf{p}n_0$ și dacă $\{\forall n \in N,\ n \geqslant n_0,\ \mathbf{p}n \Rightarrow \mathbf{p}s(n)\}$, atunci $\{\forall n \in N,\ n \geqslant n_0,\ \mathbf{p}n\}$ (*principiul II al inducției matematice*).

Într-adevăr, dacă $n_0 = 0$ se aplică direct lema 2 (principiul I al inducției matematice). Putem presupune $n_0 \neq 0$ și considerăm predicatul $\pi : N \to \mathbb{B}$ definit prin

$$\pi n = (\mathbf{p}n) \text{ sau } (n < n_0), \text{ adică}$$

$$\pi(n) = \begin{cases} \mathbf{A} \text{ dacă } \mathbf{p}(n) = \mathbf{A} \text{ sau dacă } n < n_0, \\ \mathbf{F} \text{ în caz contrar.} \end{cases}$$

Avem $\pi(0) = \mathbf{A}$, adică $\pi(0)$. Apoi, să presupunem că $\pi(n) = \mathbf{A}$. Dacă $n \geqslant n_0$, atunci în mod necesar $\mathbf{p}(n)$ $\mathbf{A}$, și, conform ipotezei din enunț, $\mathbf{p}(s(n)) = \mathbf{A}$, adică $\pi(s(n)) = \mathbf{A}$. Dacă $n < n_0$, atunci $s(n) \leqslant n_0$ conform d). În cazul cînd $s(n) < n_0$ rezultă și $\pi(s(n))$, iar dacă $s(n) = n_0$, atunci $\mathbf{p}s(n)$, deci $\pi s(n)$. Prin urmare am demonstrat că $\pi(s(n)) = \mathbf{A}$. Ca atare, conform lemei 2, rezultă că $\forall n \in N$, $\pi(n)$, deci $\forall n \geqslant n_0$, $\mathbf{p}n$.

Adăugăm acum încă două rezultate fundamentale legate de dinamici Peano.

TEOREMA 1.2. *Fie $(N, s)_0$ o dinamică Peano. În mulțimea ordonată $(N, \leqslant)$ orice parte nevidă are un cel mai mic element și orice parte nevidă majorată are un cel mai mare element.*

Demonstrație. Fie $C \subset N$ o parte nevidă și $A = \{n \in N \mid \forall m \in C,\ n \leqslant m\}$ mulțimea minoranților lui C. (v. fig. 1.9). Evident,

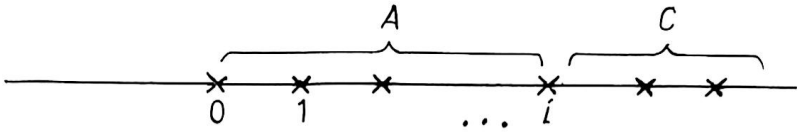


Fig. 1.9

$0 \in A$. Apoi $A \neq N$ [într-adevăr, C fiind nevidă, există $c \in C$; rezultă atunci $s(c) \notin A$ căci dacă $s(c) \in A$, $s(c)$ este un minorant al lui C, deci $s(c) \leqslant c$, ceea ce contravine proprietății b) a ordinei din N]. Conform P3, va rezulta atunci că $s(A) \not\subset A$, deci există $i \in A$ astfel încît $s(i) \notin A$. Atunci $i \in C$ [altminteri $i \notin C$ și cum $i \in A$, rezultă $i < d$ pentru orice $d \in C$. Atunci $s(i) \leqslant d$ pentru orice $d \in C$, adică $s(i) \in A$, ceea ce este absurd]. Elementul i este evident cel mai mic element al lui C.

Fie acum $D \subset N$ o parte nevidă majorată și B mulțimea (nevidă) a majoranților lui D, $B = \{n \in N \mid \forall m \in D,\ m \leqslant n\}$. Conform primei

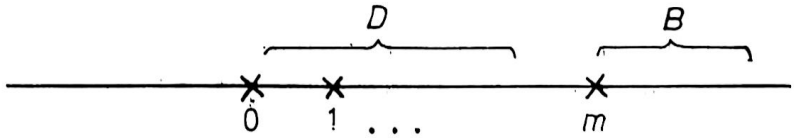


Fig. 1.10

părți a teoremei, mulțimea B are un cel mai mic element. Fie $m = \min B$. Vom arăta că $m \in D$. Dacă, prin absurd, am avea $m \notin D$, atunci $m \neq 0$ [altminteri $m = 0$ și ar rezulta că $\forall a \in D$, $a \leqslant 0$, deci $0 \in D$, ceea ce contravine faptului că $m \notin D$]. Conform lemei 1, există $m' \in N$ astfel ca $m = s(m')$. Pe de altă parte, pentru orice $a \in D$ avem $a \leqslant m'$ sau $a = m$ și din faptul că $m \notin D$ rezultă $a \leqslant m'$, deci $m' \in B$. Cum $m' < m$ se contravine faptului că $m = \min B$.

Aşadar, ipoteza că $m \notin D$ conduce la o contradicţie. Deci $m \in D$ şi prin urmare m este cel mai mare element al lui D. ∎

TEOREMA 1.3 (*teorema împărţirii cu rest*). *Fie* $(N, s)_0$ *o dinamică Peano. Pentru orice* $a, b \in N$, $b \neq 0$, *există şi sînt unice elemente* q, $r \in N$ *astfel încît*

$$a = b \cdot q + r \text{ şi } r < b.$$

Demonstraţie. Existenţa. Fixăm deci $b \in N$, $b \neq 0$ şi demonstrăm afirmaţia prin inducţie după a. Dacă $a = 0$, atunci luăm $q = 0$, $r = 0$. Presupunem proprietatea adevărată pentru elementul a şi o demonstrăm pentru succesorul său $s(a)$. Aşadar, $a = b \cdot q + r$ cu $q, r \in N$ şi $r < b$. Atunci $s(a) = b \cdot q + s(r)$ şi $s(r) \leqslant b$. Dacă am avea $s(r) = b$, atunci $s(a) = b \cdot q + b = b \cdot (q + 1) + 0$, iar dacă $s(r) < b$, atunci $s(a) = b \cdot q + s(r)$ şi proprietatea din enunţ rezultă pentru $s(a)$.

Unicitatea. Fie $q_1, r_1, q_2, r_2 \in N$ astfel încît $a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2$ şi $r_1 < b$, $r_2 < b$. Presupunem $q_1 \leqslant q_2$ (cazul $q_2 \leqslant q_1$ tratîndu-se în mod similar). Atunci $\exists\, p \in N$ astfel încît $q_1 + p = q_2$, deci $a = b \cdot q_1 + r_1 = b \cdot (q_1 + p) + r_2$, de unde $r_1 = b \cdot p + r_2$. Dacă am avea $r_1 \leqslant r_2$, atunci ar exista $p' \in N$ astfel ca $r_2 = r_1 + p'$ şi prin urmare $r_1 = b \cdot p + p' + r_1$. Aşadar, $b \cdot p + p' = 0$, de unde $p' = 0$ şi $b \cdot p = 0$, deci $r_2 = r_1$; în plus, deoarece $b \cdot p = 0$ şi $b \neq 0$, rezultă $p = 0$, adică $q_1 = q_2$. Iar dacă am avea $r_2 \leqslant r_1$, ar exista $p'' \in N$ astfel ca $r_1 = r_2 + p''$, deci $p'' \leqslant r_1 < b$ şi ca atare $p'' < b$. Atunci $r_2 + p'' = b \cdot p + r_2$, de unde $p'' = b \cdot p$. Dacă am avea $p \neq 0$, atunci $p = s(p_1)$ cu $p_1 \in N$ şi $p'' = b \cdot s(p_1) = b + b \cdot p_1 \geqslant b$, ceea ce contravine inegalităţii $p'' < b$. Rezultă în final că $p = 0$, deci $p'' = 0$ şi prin urmare $r_1 = r_2$ şi $q_1 = q_2$. ∎

Izomorfismul oricăror două dinamici Peano

Fie $(N, s)_0$ şi $(N', s')_0$, două dinamici Peano. Pe fiecare din ele considerăm operaţiile de adunare, înmulţire şi relaţia de ordine introduse anterior. Un morfism de dinamici cu iniţializare

$$f : (N, s)_0 \to (N', s')_0'$$

adică o aplicaţie $f : N \to N'$, astfel încît $f \circ s = s' \circ f$ şi $f(0) = 0'$, se numeşte *izomorfism algebric* dacă:

a) f este bijectivă;

b) $\forall\, m, n \in N$, $f(m + n) = f(m) + f(n)$ şi $f(m \cdot n) = f(m) \cdot f(n)$;

c) f este izotonă (adică $\forall\, m, n \in N$, $m \leqslant n \Rightarrow f(m) \leqslant f(n)$).

Dacă există un astfel de izomorfism algebric, se mai spune că dinamicile considerate sînt *algebric izomorfe*.

TEOREMA 1.4. *Orice două dinamici Peano sînt algebric izomorfe.*

Demonstrație. Fie $(N, s)_0$ și $(N', s')_{0'}$ două dinamici Peano arbitrare. Conform teoremei 1.1, există și este unic un morfism de dinamici cu inițializare $f : (N, s)_0 \to (N', s')_{0'}$. De asemenea, există și este unic un morfism similar $g : (N', s')_{0'} \to (N, s)_0$. Morfismele $g \circ f$ și 1_N de la $(N, s)_0$ la $(N', s')_{0'}$ au ambele o aceeași proprietate; anume, $(g \circ f) \circ s = g \circ (f \circ s) = g \circ (s' \circ) = (g \circ s') \circ f$ $(s \circ g)$ $f = s \circ$ $\circ (g \circ f)$, $1_N \circ s = s \circ 1_N = s$, $(g \circ f)(0) = g(f(0))$ $g(0') = 0$ și $1_N(0) =$ $= 0$. Atunci $g \circ f = 1_N$. În mod analog $f \circ g = 1_{N'}$. De aici rezultă că f este aplicație bijectivă.

Prin inducție după n se demonstrează cu ușurință că $\forall\, m, n \in N$, $f(m + n) = f(m) + f(n)$ și utilizînd acest fapt rezultă că $f(m \cdot n) = f(m) \cdot f(n)$.

Dacă $m, n \in N$ și $m \leqslant n$, atunci există $p \in N$ astfel ca $m + p = n$, deci $f(m + p) = f(n)$. Așadar, $f(m) + f(p)$ $f(n)$ și în consecință $f(m) \leqslant f(n)$. ∎

Din acest moment vom fixa o dinamică Peano $(N, s)_0$ pe care o vom nota pe scurt cu $\mathbb{N}$. Elementele mulțimii suport $\mathbb{N}$ se vor numi *numere naturale*; elementul inițial $0 \in \mathbb{N}$ se numește *zero*, iar aplicația $s : \mathbb{N} \to \mathbb{N}$, $n \mapsto s(n) = n + 1$ este *funcția-succesor*. Se introduc succesiv numerele naturale

$$1 = s(0),\ 2 = s(1),\ 3 = s(2) \text{ etc.}$$

Desigur, trebuie distins între un număr natural și notația care îl reprezintă. De exemplu, elementele lui $\mathbb{N}$ pot fi notate în diverse moduri: $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, $\mathbb{N} = \{\text{zero, unu, doi, trei}, \ldots\}$, $\mathbb{N} =$ $= \{0, 01, 011, 0111, \ldots\}$ etc. Ideea de bază constă în a fixa un element inițial și a indica pentru orice element succesorul lui. Proprietățile P1—P3 ale lui Peano esențializează intuiția noastră despre numere naturale și constituie un punct principal în fundamentarea matematicii discrete.

Faptul că au fost folosite anterior acestui moment numerele naturale (inclusiv la numerotarea paginilor de pînă acum ale cărții!) nu este un viciu de fond.

Orice dinamică Peano este algebric izomorfă cu $\mathbb{N}$ (conform teoremei 1.4) astfel că toate rezultatele anterioare au loc pentru mulțimea $\mathbb{N}$ și le vom aplica în continuare ca atare. De exemplu, $\mathbb{N}$ satisface prin definiție proprietățile P1—P3 și are loc principiul inducției matematice (lema 2). De asemenea, este valabilă teorema de inițialitate (teorema 1.1), pe care o vom aplica în continuare; anume, *pentru orice triplet* (M, φ, a) *format dintr-o mulțime* M, *o aplicație* $\varphi : M \to M$ *și un element* $a \in M$, *există și este unică o aplicație de mulțimi* $f : \mathbb{N} \to M$ *astfel încît* $\varphi \circ f = f \circ s$ *și* $f(0) = a$.

Inducția matematică permite demonstrarea în două etape a proprietăților referitoare la numere naturale. Dar, mai mult, anumite obiecte pot fi definite prin inducție (sau, cum se mai spune, recursiv).

De exemplu, funcția factorial $f : \mathbb{N} \to \mathbb{N}$, $f(n) = n!$ poate fi definită în mai multe moduri :

— *direct*, punînd $\forall\, n \in \mathbb{N}$, $f(n) \begin{cases} 1 & \text{dacă } n = 0, \\ 1 \cdot 2 \cdot \ldots \cdot n & \text{dacă } n \geqslant 1. \end{cases}$

— *recursiv* : se pune $f(0) = 1$ (baza inducției) și $f(n+1) = (n+1) \cdot f(n)$ (pasul de inducție).

— *printr-un program de calcul* : N ! IF N 0 THEN 1 ELSE N*(N − 1)! (așadar, dacă n 0, atunci $n!$ 1 ; iar dacă $n \neq 0$, atunci valoarea lui $n!$ este $n \cdot (n$ 1)! și calculul se reia pentru $(n-1)!$ etc.).

Aplicații

a) *Reprezentarea zecimală a numerelor naturale.* Să notăm $K = \{0, 1, 2, \ldots, 9\}$ mulțimea cifrelor zecimale. Vom defini o dinamică cu inițializare N_K în modul următor. Un element x din N_K este fie o cifră zecimală (din K), fie de forma yt (juxtapunere și nu înmulțire), cu $y \in N_K$ și $t \in K$.

Exemplu. $1984 \in N_K$ deoarece succesiv 1, 19, 198, 1984 aparțin lui N_K.

Pentru orice $n \in K$, notăm $n' = \begin{cases} n+1 & \text{dacă } 0 \leqslant n \leqslant 8, \\ 0 & \text{dacă } n = 9 \end{cases}$

și definim recursiv funcția $s : N_K \to N_K$ astfel :

— dacă $x \in K$, punem $s(x) = \begin{cases} x' & \text{dacă } 0 \leqslant x \leqslant 8, \\ 10 & \text{dacă } x = 9 ; \end{cases}$

— dacă $x = yt$ cu $y \in N_K$, $t \in K$, punem $s(x) = \begin{cases} yt' & \text{dacă } 0 \leqslant t \leqslant 8 \\ s(y)0 & \text{dacă } t = 9. \end{cases}$

Exemple. Avem $7' = 8$, $9' = 0$, $s(7) = 8$, $s(9) = 10$. Dacă $x = 1984$, atunci $x = yt$ cu $y = 198$ și $t = 4$, deci $s(1984) = 1985$, iar dacă $x = 1999$, atunci $x = yt$ cu $y = 199$ și $t = 9$, deci $s(1999) = s(199)0$. Dar $s(199) = s(19)0$ iar $s(19) = 20$, deci $s(1999) = 2000$.

Am definit astfel o dinamică cu inițializare $(N_K, s)_0$, care verifică proprietățile P1, P2, P3. Conform teoremei 1.4 există un izomorfism algebric $f : \mathbb{N} \to N_K$. Pentru orice număr natural $n \in \mathbb{N}$, $f(n)$ este *reprezentarea zecimală* a lui n.

Vom generaliza (și totodată vom formaliza mai riguros) această construcție în legătură cu definirea cuvintelor peste un alfabet oarecare.

b) Fie M o mulțime fixată și $\rho \in \mathrm{Rel}\, M$ o relație binară pe M. Se definesc inductiv pentru orice $n \in \mathbb{N}$ relațiile binare $\rho^n \in \mathrm{Rel}\, M$ în modul următor:

$$\rho^0 = 1_M,\ \rho^1 = \rho,\ \rho^2 = \rho \circ \rho \text{ și } \rho^{n+1} = \rho^n \circ \rho.$$

[Se poate considera dinamica cu inițializare $(\mathrm{Rel}\, M, \varphi)_M$, unde $\varphi : \mathrm{Rel}\, M \to \mathrm{Rel}\, M$, $\sigma \mapsto \sigma \circ \rho$ și aplicînd teorema 1.1 de inițialitate, există un morfism de dinamici $p_\rho : \mathbb{N} \to \mathrm{Rel}\, M$ astfel încît $p_\rho \circ s = \varphi \circ p_\rho$ și $p_\rho(0) = 1_M$. Se notează atunci $\rho^n = p_\rho(n)$ etc.] Avem $x \rho^0 y \leftrightarrow x = y$; pentru $n \geqslant 2$, $\forall\, x, y \in M$, $x \rho^n y \leftrightarrow \exists\, u_1, \ldots, u_{n-1} \in M$ astfel încît $x \rho u_1$, $u_1 \rho u_2, \ldots, u_{n-1} \rho y$. Avem $\forall\, m, n \in \mathbb{N}$. $\rho^{m+n} = \rho^m \circ \rho^n$. Dacă ρ este o relație tranzitivă, atunci $\rho^n \subset \rho$ pentru orice $n \in \mathbb{N}$.

Să considerăm acum relația

$$\rho^* = \bigcup_{n \geqslant 0} \rho^n.$$

Așadar, $\forall\, x, y \in M$, $x \rho^* y \leftrightarrow \exists\, n \in \mathbb{N}$ astfel încît $x \rho^n y$. Relația ρ^* este reflexivă deoarece $\forall\, x \in M$ avem $(x, x) \in 1_M$, deci $(x, x) \in \rho^0$ și ca atare $(x, x) \in \rho^*$. Apoi relația ρ^* este tranzitivă: dacă $x \rho^* y$ și $y \rho^* z$, atunci $\exists\, m, n \geqslant 0$ astfel încît $x \rho^m y$ și $y \rho^n z$, deci $x \rho^{m+n} z$, adică $(x, z) \in \rho^{m+n}$. Așadar, $(x, z) \in \rho^*$, adică $x \rho^* z$. Relația binară ρ^* este numită *închiderea reflexivă și tranzitivă* a lui ρ (sau, echivalent, *preordinea pe M asociată lui ρ*).

Mulțimea $\mathrm{Rel}\, M = \mathbf{p}(M^2)$ este ordonată relativ la incluziune. Dacă $\rho \in \mathrm{Rel}\, M$, atunci ρ^* este *cea mai mică* relație de preordine care conține ρ. Într-adevăr, avem $\rho \subset \rho^*$ și dacă ρ_1 este o relație de preordine pe M astfel încît $\rho \subset \rho_1$, atunci $\rho^* \subset \rho_1$ [dacă $(x, y) \in \rho^*$, atunci sau $x = y$ și ca atare $(x, y) \in \rho_1$ sau există $n \geqslant 1$ astfel ca $x \rho^n y$, deci $x \rho_1^n y$, adică $x \rho_1 y$]. În mod similar, relația

$$\rho^+ = \bigcup_{n > 0} \rho^n$$

este cea mai mică relație tranzitivă care conține ρ și se numește *închiderea tranzitivă* a lui ρ.

Exemplu. Fie $M = \mathbb{N}$ și relația binară $\rho \in \mathrm{Rel}\, \mathbb{N}$ definită prin $x \rho y \leftrightarrow y = x + 1$. În acest caz $\rho^* = „\leqslant"$ iar $\rho^+ = „<"$.

c) Fixăm o dinamică $(M, \varphi)_a$ cu inițializare. Conform teoremei 1.1 de inițialitate, există și este unică o aplicație $f_a : \mathbb{N} \to M$ astfel încît $\varphi \circ f_a = f_a \circ s$ și $f_a(0) = a$. Arătăm mai întîi că $\bar{a} = f_a(\mathbb{N})$

Într-adevăr, dacă $x \in f_a(\mathbb{N})$, atunci $x = f_a(n)$ cu $n \in \mathbb{N}$, deci $\varphi(n) = \varphi(f_a(n)) = f_a(s(n)) = f_a(n+1) \in f_a(\mathbb{N})$. Apoi $a = f_a(0) \in f_a(\mathbb{N})$. Aşadar, $f_a(\mathbb{N})$ este o subdinamică ce conţine a. Rămîne să arătăm că este cea mai mică subdinamică cu această proprietate; or, dacă $S \subset M$ este o altă subdinamică ce conţine a, atunci se arată uşor, prin inducţie după n, că $\forall\, n \in \mathbb{N}$, $f_a(n) \in S$, adică $f_a(\mathbb{N}) \subset S$.

Mulţimea M^M a tuturor funcţiilor totale de la M la M se poate considera ca dinamică prin considerarea aplicaţiei $\Phi : M^M \to M^M$, $h \mapsto \varphi \circ h$. Teorema de iniţialitate arată că există şi este unică o aplicaţie

$$p_\varphi : \mathbb{N} \to M^M \text{ astfel încît } p_\varphi(0) = 1_M.$$

Pentru orice $n \in \mathbb{N}$ se notează $p_\varphi(n)$ cu φ^n; aşadar,

$$\varphi^0 = 1_M,\ \varphi^{n+1} = \varphi \circ \varphi^n \text{ (deci } \varphi^n = \overbrace{\varphi \circ \ldots \circ \varphi}^{n \text{ ori}}).$$

Pentru orice dinamică $(M, \varphi)_a$ cu iniţializare se poate defini *aplicaţia de evaluare în* a

$$\mathrm{ev}_a : M^M \to M, \quad h \mapsto h(a),$$

care este un morfism de dinamici cu iniţializare, deoarece $\forall\, h \in M^M$

$$\mathrm{ev}_a(\Phi(h)) = \mathrm{ev}_a(\varphi \circ h) = (\varphi \circ h)(a) = \varphi(h(a)) = \varphi(\mathrm{ev}_a(h)),$$

adică $\mathrm{ev}_a \circ \Phi = \varphi \circ \mathrm{ev}_a$ şi, în plus, $\mathrm{ev}_a(1_M) = 1_M(a) = a$. Atunci rezultă că $\mathrm{ev}_a \circ p_\varphi : \mathbb{N} \to M$ este de asemenea un morfism de dinamici şi, în plus, $(\mathrm{ev}_a \circ p_\varphi)(0) = a$. Aşadar, $\mathrm{ev}_a \circ p_\varphi$ şi f_a sînt morfisme de dinamici $\mathbb{N} \to M$ avînd aceeaşi valoare în 0 şi din unicitatea lui f rezultă că $\mathrm{ev}_a \circ p_\varphi = f_a$. De aici rezultă următoarea lemă.

LEMA 3. *Dacă* $(M, \varphi)_a$ *este o dinamică cu iniţializare, atunci* $\forall\, n \in \mathbb{N}$, $f_a(n) = \varphi^n(a)$ *şi, în plus,* $\bar{a} = \{\varphi^n(a) \mid n \in \mathbb{N}\}$.

Demonstraţie. Avem $f_a(n) = (\mathrm{ev}_a \circ p_\varphi)(n) = \mathrm{ev}_a(p_\varphi(n)) = \mathrm{ev}_a(\varphi^n) = \varphi^n(a)$; apoi

$$\bar{a} = f_a(\mathbb{N}) = \{f_a(n) \mid n \in \mathbb{N}\} = \{\varphi^n(a) \mid n \in \mathbb{N}\}. \blacksquare$$

Exemplu. Pentru dinamica Peano $(\mathbb{N}, s)_0$ avem evident $\overline{0} = \mathbb{N}$ (conform P3), deci $\mathbb{N} = \{s^n(0) \mid n \in \mathbb{N}\}$, un rezultat aşteptat.

Reamintim că două dinamici cu iniţializare $(M_1, \varphi_1)_{a_1}$, $(M_2, \varphi_2)_{a_2}$ se numesc *izomorfe* dacă există o aplicaţie bijectivă $f : M_1 \to M_2$ astfel încît $f \circ \varphi_1 = \varphi_2 \circ f$ şi $f(a_1) = a_2$.

Pentru orice $p \in \mathbb{N}$, $p \geqslant 1$, notăm $S_p = \{0, 1, \ldots, p-1\}$ și considerăm aplicația $t_k : S_p \to S_p$ ($0 \leqslant k < p$ fixat), definită prin :

$$t_k(x) = \begin{cases} x+1 & \text{dacă } 0 \leqslant x < p-1, \\ k & \text{dacă } x = p-1. \end{cases}$$

Atunci $(S_p, t_k)_0$ este o dinamică cu inițializare.

TEOREMA 1.5 (*Dedekind*). *Fie (M, φ) o dinamică astfel încît să existe un element $a \in M$ cu proprietatea că $\bar{a} = M$. Atunci dinamica $(M, \varphi)_a$ este izomorfă cu una din următoarele două dinamici : $(\mathbb{N}, s)_0$; $(S_p, t_k)_0$ cu $p \geqslant 1$, $0 \leqslant k < p$, convenabili.*

Demonstrație. Considerăm morfismul de dinamici cu inițializare $f_a : (\mathbb{N}, s)_0 \to (M, \varphi)_a$. Conform lemei 3 avem $M = \{\varphi^n(a) \; n \in \mathbb{N}\}$ și $\forall\, n \in \mathbb{N}$, $f_a(n) = \varphi^n(a)$. Din ipoteza $\bar{a} = M$, rezultă că aplicația f_a : $: \mathbb{N} \to M$ este surjectivă. Apar două cazuri :

I) Dacă toate elementele $\varphi^n(a)$, $n \in \mathbb{N}$, sînt distincte două cîte două, atunci aplicația f_a este injectivă, deci bijectivă și $(M, \varphi)_a$ este izomorfă cu $(\mathbb{N}, s)_0$; în figura 1.11 este sugerată structura elementelor mulțimii M.

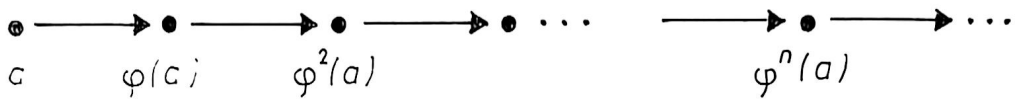


Fig. 1.11

II) Dacă nu toate elementele $\varphi^n(a)$, $n \geqslant 0$, sînt distincte, atunci conform teoremei 1.2 există $p \in \mathbb{N}$, $p \geqslant 1$, minim astfel încît să existe $k < p$ cu proprietatea că $\varphi^k(a) = \varphi^p(a)$. Prin inducție după r, se verifică imediat că $\varphi^{k+r}(a) = \varphi^{p+r}(a)$ pentru orice $r \in \mathbb{N}$, deci $\varphi^{(q+1)p-qk+r}(a) = \varphi^{k+r}(a)$ pentru orice $q \in \mathbb{N}$.

Să considerăm aplicația de restricție $g = f_a | S_p$, $g : S_p \to M$. Arătăm că $\varphi \circ g = g \circ t_k$ [într-adevăr, $\forall\, x \in S_p$, $\varphi(g(x)) = \varphi(f_a(x)) = \varphi(\varphi^x(a)) = \varphi^{x+1}(a)$ și, pe de altă parte, dacă $0 \leqslant x < p-1$, $g(t_k(x)) = f_a(t_k(x)) = f_a(x+1) = \varphi^{x+1}(a)$, iar dacă $x = p-1$, atunci $g(t_k(x)) = g(k) = f_a(k) = \varphi^k(a) = \varphi^p(a) = \varphi^{x+1}(a)$] ; de asemenea, $g(0) = f_a(0) = a$, deci g este un morfism de dinamici cu inițializare.

Apoi, g este surjectivă [pentru că $\forall\, x \in M$, $\exists\, n \in \mathbb{N}$ astfel ca $x = f_a(n) = \varphi^n(a)$. Împărțim $n-p$ la $p-k$ (teorema 1.3) și există $q, r \in \mathbb{N}$ astfel ca $n - p = q(p-k) + r$, $r < p-k$; atunci $(q+1)p - qk \leqslant n < (q+2)p - (q+1)k$ și $\varphi^n(a) = \varphi^{(q+1)p-qk+r}(a) = \varphi^{k+r}(a)$ cu $k + r < p$, deci $x = \varphi^{k+r}(a) = f_a(k+r)$ și ca atare $x = g(k+r)$ cu $k + r \in S_p$] ; în fine, arătăm că g este injectivă : dacă $g(u) = g(v)$ cu $u, v \in S_p$, rezultă $\varphi^u(a) = \varphi^v(a)$, deci în mod necesar

$u = v$ pentru că altfel s-ar nega minimalitatea lui p. În concluzie, aplicația g stabilește un izomorfism de dinamici cu inițializare de la $(S_p, t_k)_0$ la $(M, \varphi)_a$ (v. fig. 1.12).■

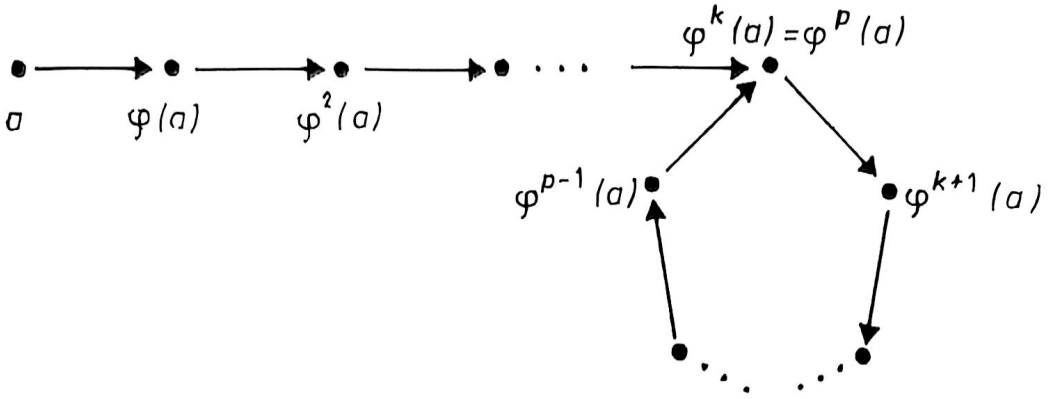


Fig. 1.12

O dinamică $(M, \varphi)_a$ cu proprietatea $\bar{a} = M$ se mai numește *dinamică generată de elementul a*. Teorema 1.5 clasifică în mod complet aceste dinamici iar fig. 1.11 și 1.12 sugerează caracterul liniar și respectiv ciclic al dinamicilor respective.

Clasificarea dinamicilor evolutive

Să fixăm o dinamică (M, φ) cu M nevidă (definiția 1.5); $\forall\, a \in M$, $\bar{a} = \{\varphi^n(a) \mid n \in \mathbb{N}\}$. Pe mulțimea M se poate considera relația de preordine:

$$a \leqslant b \leftrightarrow \bar{b} \subset \bar{a}.$$

Așadar, $a \leqslant b \leftrightarrow b \in \bar{a} \leftrightarrow \exists\, n \in \mathbb{N}, b = \varphi^n(a)$. Dinamica (M, φ) se numește *evolutivă* dacă această preordine este totală, adică $\forall\, u, v \in M$, sau $u \leqslant v$, sau $v \leqslant u$. În acest caz vom nota cu S, respectiv I, submulțimea lui M a majoranților (resp. minoranților) lui M.

Exemple. Următoarele dinamici sînt evolutive (v. fig. 1.13):

(i) $(\mathbb{N}, s)$, unde $s : \mathbb{N} \to \mathbb{N}$, $n \mapsto n + 1$; aici $S = \emptyset$, $I = \{0\}$.

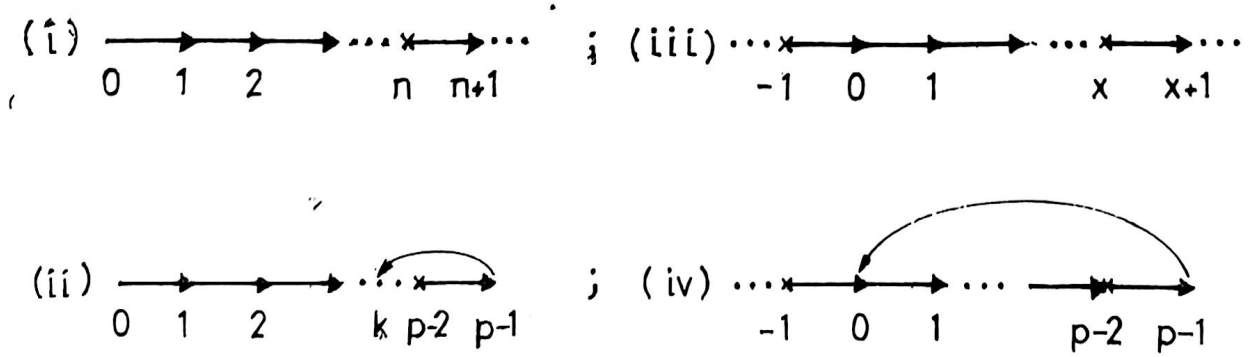


Fig. 1.13

(ii) Fixăm $p \geqslant 1$ întreg și $0 \leqslant k < p$. Atunci (S_p, t_k) este o dinamică evolutivă cu I și S nevide.

(iii) $(\mathbb{Z}, s)$, unde $s : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x + 1$; aici $S = \emptyset$, $I = \emptyset$.

(iv) Fie $M = \{x \in \mathbb{Z} \mid x < p\}$ cu $p \geqslant 1$ fixat și $\varphi : M \to M$, $\varphi(x) = x + 1$, dacă $x < p - 1$ și $\varphi(p - 1) = 0$. Atunci (M, φ) este o dinamică evolutivă pentru care $I = \emptyset$, $S \neq \emptyset$.

Folosind teorema 1.5, vom arăta că *orice dinamică evolutivă este izomorfă cu una din dinamicile* (i) — (iv) *precedente*. Subliniem doar ideea demonstrației ([40]). Fie (M, φ) o dinamică evolutivă și S, respectiv I, mulțimea majoranților (resp. minoranților) lui M. Dacă $I \neq \emptyset$ și $a \in I$, atunci $\forall\, x \in M$, $a \leqslant x$, deci $x \in \bar{a}$ și prin urmare $M = \bar{a}$. Conform teoremei 1.5, dinamica (M, φ) este izomorfă cu una din dinamicile (i), (ii). Dacă $I = \emptyset$, $S = \emptyset$, atunci (M, φ) este izomorfă cu $(\mathbb{Z}, s)$ și rămîne de analizat cazul cînd $I = \emptyset$, $S \neq \emptyset$. Alegem atunci un element $s \in S$. Așadar, $\varphi(s) \leqslant s$ și fie p cel mai mic număr natural nenul astfel ca $s = \varphi^p(s)$. Pentru orice $x \in S$, există și este unic k, $0 \leqslant k < p$, astfel încît $x = \varphi^k(s)$ [într-adevăr, avem $s \leqslant x$ și prin urmare $x = \varphi^m(s)$ cu $m \in \mathbb{N}$. Dar $m = p \cdot u + k$ cu $u, k \in \mathbb{N}$, $k < p$, deci $x = \varphi^k(s)$; pentru unicitate, dacă $x = \varphi^k(s) = \varphi^{k_1}(s)$ și $0 \leqslant k < k_1 < p$, atunci $\varphi^{p-k_1+k}(s) = \varphi^{p-k_1}(\varphi^k(s)) = \varphi^{p-k_1}(\varphi^{k_1}(s)) = \varphi^p(s) = s$ și deoarece $p - k_1 + k < p$, s-ar nega alegerea lui p]. Așadar, mulțimea S are exact p elemente. Pe de altă parte, avem $S \neq M$ (căci dacă $S = M$, atunci $M = I = \emptyset$, absurd). Prin urmare putem alege un element $z \in M \setminus S$. Deoarece dinamica (M, φ) este evolutivă, rezultă că există $n = \min\{k \in \mathbb{N} \mid \varphi^k(z) \in S\}$. Avem, evident, $n \geqslant 1$ și notăm $a = \varphi^n(z)$. Se arată ușor că a nu depinde de alegerea lui z, că $\forall\, x \in M \setminus S$, există și este unic $m(x)$ astfel ca $\varphi^{m(x)}(x) = a$ și că $\forall\, x \in S$, există și este unic $0 \leqslant n(x) < x$, astfel ca $\varphi^{p-n(x)}(x) = a$. Luînd $M_1 = \{x \in \mathbb{Z} \mid x < p\}$ și aplicația $\varphi_1 : M_1 \to M_1$, $\varphi_1(x) = x + 1$ dacă $x < p - 1$ și $\varphi_1(p - 1) = 0$, atunci aplicația

$$f = M \to M_1,\ f(x) = \begin{cases} -m(x) & \text{dacă } x \in M \setminus S, \\ n(x) & \text{dacă } x \in S \end{cases}$$

este bijectivă cu $\varphi_1 \circ f = f \circ \varphi$, deci este un izomorfism de dinamici.

§ 1.3. RELAȚII, PREDICATE ȘI OPERAȚII ALGEBRICE n-ARE ($n \in \mathbb{N}$)

Puteri carteziene

Pentru orice număr natural $n \geqslant 1$ notăm $S_n = \{0, 1, \ldots, n - 1\}$; definim de asemenea $S_0 = \emptyset$.

Fie $M_1, \ldots, M_n$ mulțimi din universul $\mathcal{U}$. Reamintim că $\bigcup_{i=1}^{n} M_i = \{x \mid \exists i, x \in M_i\}$, $\bigcap_{i=1}^{n} M_i = \{x \mid \forall i, x \in M_i\}$ și $\sum_{i=1}^{n} M_i = \bigcup_{i=1}^{n} (M_i \times \{i\})$.

Orice funcție totală $f : S_n \to \bigcup_{k=1}^{n} M_k$ astfel încît $f(0) \in M_1, \ldots, f(n-1) \in M_n$ se numește *sistem ordonat* de elemente din $M_1, \ldots, M_n$; notînd $a_k = f(k-1)$, $1 \leqslant k \leqslant n$, un astfel de sistem ordonat se mai notează $(a_1, \ldots, a_n)$.

Două sisteme ordonate $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n)$ sînt *egale* dacă și numai dacă $a_1 = b_1$ în $M_1, \ldots, a_n = b_n$ în M_n. În acest mod este generalizată noțiunea de pereche ordonată.

Mulțimea tuturor sistemelor ordonate $(a_1, \ldots, a_n)$ cu $a_1 \in M_1, \ldots, a_n \in M_n$ este numită *produsul cartezian* al mulțimilor $M_1, \ldots, M_n$ și este notată cu

$$\prod_{k=1}^{n} M_k = M_1 \times \ldots \times M_n.$$

Un produs cartezian de mulțimi este vid dacă și numai dacă cel puțin una dintre mulțimi este vidă; pentru $n = 2$ se regăsește produsul cartezian $M_1 \times M_2$ definit în § 1.1.

Fie M o mulțime și $n \geqslant 1$ natural. Se notează cu M^n produsul cartezian a n exemplare ale mulțimii M, adică

$$M^n = \prod_{k=1}^{n} M_k, \text{ unde } M_1 = \ldots = M_n = M.$$

Așadar, M^n este mulțimea tuturor aplicațiilor $S_n \to M$. Orice element din M^n este un sistem ordonat $c = (a_1, \ldots, a_n)$ de elemente din M și se mai numește *șir finit în* M (sau, echivalent, *cuvînt de lungime n cu litere din* M); uneori se scrie $c = a_1 \ldots a_n$ omițînd parantezele și virgulele.

Se pune, prin definiție, $M^0 = \mathbb{1}$, prototipul mulțimii avînd un singur element; acesta este uneori notat cu $\wedge_M$ și se numește *cuvîntul vid în* M, considerat de lungime zero.

Exemple. Fie $\mathbb{B} = \{0, 1\}$ codul binar. Atunci $\mathbb{B}^0 = \{\wedge_{\mathbb{B}}\}$, $\mathbb{B}^1 = \mathbb{B}$, $\mathbb{B}^2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$. Elementele lui $\mathbb{B}^n$, $n \geqslant 1$, se mai numesc *cuvinte binare de lungime n* (sau *șiruri de n biți*).

Relații și predicate n-are

DEFINIȚIA 1.7. Fie $n \in \mathbb{N}$, $n \geqslant 1$. Se numește *relație n-ară* (sau *relație de aritate n*) orice sistem ordonat

$$\rho = (M_1, \ldots, M_n, R)$$

format din n mulțimi $M_1, \ldots, M_n$ și o parte R a produsului lor cartezian, $R \subset M_1 \times \ldots \times M_n$ (numită *graficul* relației ρ).

Dacă $M_1 = \ldots = M_n = M$, atunci $R \subset M^n$; se scrie $\rho = (M, n, R)$ și se spune că ρ este o *relație n-ară pe* M. O relație n-ară pe M este evident o relație unară pe M^n.

Dacă $x_1 \in M_1, \ldots, x_n \in M_n$ și dacă $(x_1, \ldots, x_n) \in R$, atunci se mai spune că elementele $x_1, \ldots, x_n$ sînt în relația ρ (sau R) și se mai scrie $\rho(x_1, \ldots, x_n)$. Pentru $R = \emptyset$ se obține relația *vidă*. Pentru $n = 1$ relațiile 1-are pe o mulțime M se numesc *unare* și ele se identifică cu părțile lui M. Pentru $n = 2, 3, \ldots$ se obțin relațiile *binare*, *ternare* etc.

Exemplu. Mulțimea $\{x^2 + y^2 = z^2\}$ definește o relație ternară pe $\mathbb{Z}$. Formal aceasta este $\rho = (\mathbb{Z}, 3, R)$, unde $R = \{(x, y, z) \in \mathbb{Z}^3 \mid x^2 + y^2 = z^2\}$.

Dacă ρ_1, ρ_2 sînt două relații pe aceleași mulțimi și avînd aceeași aritate, atunci se pot defini în mod natural *intersecția* $\rho_1 \cap \rho_2$, *reuniunea* $\rho_1 \cup \rho_2$, *complementara* $\overline{\rho}_1$ a lui ρ_1. În omogenizarea aritații, în calcule cu mai multe relații este utilă *adăugarea unei coordonate fictive*. Anume, fie $\rho = (M_1, \ldots, M_n, R)$ o relație n-ară; dacă M este o mulțime, atunci se poate considera relația $(n+1)$-ară $\nabla \rho$,

$$\nabla \rho = (M, M_1, \ldots, M_n, \nabla R),$$

unde $\forall a \in M, x_1 \in M_1, \ldots, x_n \in M_n$, $\nabla R(a, x_1, \ldots, x_n) \leftrightarrow R(x_1, \ldots, x_n)$.

Exemplu. Pe mulțimea $\mathbb{B}^3$ se consideră relația ρ definită prin $R = \{(x, y, z) \mid x = y = z\}$. Atunci pe mulțimea $M \times \mathbb{B}^3$ se poate considera relația $\nabla\rho$ punînd

$$\forall a \in M, \ \forall x, y, z \in \mathbb{B}, \ \nabla R(a, x, y, z) \leftrightarrow x = y = z.$$

Definim acum compunerea relațiilor. Fie $\rho = (M_1, \ldots, M_{n-1}, M, R)$ o relație n-ară și $\rho' = (M, M_n, M_{n+1}, \ldots, M_{n+m-2}, S)$ o relație m-ară, mulțimea M fiind „puntea de legătură" între ρ și ρ'. Atunci se poate defini *relația compusă* $\rho' \circ \rho$ ca fiind relația $(n + m - 2)$-ară

$$\rho' \circ \rho = (M_1, M_2, \ldots, M_{n+m-2}, S \circ R),$$

unde

$$S \circ R = \{(x_1, x_2, \ldots, x_{n+m-2}) \mid \exists\, u \in M \text{ astfel ca } (x_1, x_2, \ldots, x_{n-1}, u) \in R$$
$$\text{și } (u, x_n, x_{n+1}, \ldots, x_{n+m-2}) \in S\}.$$

Operația de compunere este asociativă, dar nu și comutativă. În cazul $n = m = 2$ regăsim compunerea relațiilor binare.

Relațiile n-are funcționale modelează funcțiile de mai multe variabile. O relație n-ară $\rho = (M_1, \ldots, M_n, R)$, $n \geqslant 2$ se numește *funcție parțială* (resp. *totală*),

$$R : M_1 \times \ldots \times M_{n-1} \to M_n,$$

dacă $\forall (x_1, \ldots, x_{n-1}) \in M_1 \times \ldots \times M_{n-1}$, există cel mult un element (resp. exact un element) $x_n \in M_n$ astfel încît $R(x_1, \ldots, x_{n-1}, x_n)$.

DEFINIȚIA 1.8. Fie $n \geqslant 1$ și $A_1, \ldots, A_n$ mulțimi fixate. Se numește *predicat* n-ar (sau *condiție* relativ la sistemele de elemente din mulțimile $A_1, \ldots, A_n$) orice funcție

$$\mathbf{p} : A_1 \times \ldots \times A_n \to \mathbb{B}, \quad \mathbb{B} = \{\mathbf{F}, \mathbf{A}\}.$$

Mulțimea

$$M_{\mathbf{p}} = \{(a_1, \ldots, a_n) \in A_1 \times \ldots \times A_n \mid \mathbf{p}(a_1, \ldots, a_n) = \mathbf{A}\}$$

se numește *mulțimea de adevăr a predicatului* p. În cazul cînd $(a_1, \ldots, a_n) \in M_{\mathbf{p}}$, se mai scrie $\mathbf{p}(a_1, \ldots, a_n)$ și se mai spune că p *este adevărat* pe sistemul ordonat $(a_1, \ldots, a_n)$. Numărul n se numește *ordinul de aritate* al predicatului $\mathbf{p}$.

Dacă $A_1 = \ldots = A_n = A$, orice funcție $\mathbf{p} : A^n \to \mathbb{B}$ se mai numește *predicat n-ar pe mulțimea A*. Mulțimea sa de adevăr este evident o relație n-ară pe A.

A da un predicat *nular* (de ordin $n = 0$) pe o mulțime A, adică o funcție $A^0 \to \mathbb{B}$ revine la a fixa un element din B (deoarece $A^0 = \mathbb{1}$).

Exemplu. Fie $A = \mathbb{Z}$. Predicatul binar de egalitate în $\mathbb{Z}$ este funcția

$$\mathbf{p} : \mathbb{Z}^2 \to \mathbb{B}, \quad \mathbf{p}(x, y) = \begin{cases} \mathbf{A} \text{ dacă } x = y, \\ \mathbf{F} \text{ dacă } x \neq y. \end{cases}$$

Mulțimea de adevăr este $M_{\mathbf{p}} = \{(x, x) \in \mathbb{Z}^2 \mid x \in \mathbb{Z}\}$.

Interpretare sistemică

Relațiile n-are de tipul $\rho = (M_1, \ldots, M_n, R)$ modelează *sistemele multivariabile* (cu mai multe intrări sau ieșiri). Un *multiport electric*, mai precis un n-port pe un interval de timp $\mathcal{T}$ este o relație binară (I, U, P), unde I este mulțimea curenților $i : \mathcal{T} \to \mathbb{R}^n$, U este mulțimea tensiunilor $u : \mathcal{T} \to \mathbb{R}^n$, iar P este o colecție de perechi $(i, u) \in I \times U$ supuse la diverse constrîngeri de tip fizic (sau matematic exprimînd, de exemplu, apartenența funcțiilor i, u la o clasă particulară de funcții). Deoarece avem o corespondență bijectivă $(\mathbb{R}^n)^{\mathcal{T}} \to$

$\mathbb{R}^{\mathcal{S}} \times \ldots \times \mathbb{R}^{\mathcal{S}}$, care asociază fiecărei funcții $\varphi : \mathcal{S} \to \mathbb{R}^n$ sistemul ordonat al celor n componente ale lui φ, un n-port este o relație $2n$-ară pe mulțimea $\mathbb{R}^{\mathcal{S}}$.

Operații algebrice n-are

DEFINIȚIA 1.9. Fie M o mulțime fixată și $n \in \mathbb{N}$. Se numește *operație algebrică n-ară pe M* (sau *lege de compoziție internă pe M având ordinul de aritate n*) orice funcție totală $f : M^n \to M$. [Așadar, pentru orice $x_1, \ldots, x_n \in M$ este asociat un element bine determinat $f(x_1, \ldots, x_n)$ din M]. Uneori f se mai numește *eticheta* operației.

Pentru $n = 2$ se regăsesc operațiile binare. Dacă $* : M^2 \to M$ este o astfel de operație și dacă $x, y \in M$, atunci se mai scrie $x * y$ în loc de $*(x, y)$. O operație *unară* ($n = 1$) pe o mulțime M este o funcție $f : M \to M$. Apoi o operație *nulară* ($n = 0$), adică o funcție $\mathbb{1} \to M$ revine la a fixa un element din M.

Exemplu. Fie $M = \mathbb{Z}$. Adunarea $+ : \mathbb{Z}^2 \to \mathbb{Z}$, $(x, y) \mapsto x + y$, înmulțirea $\cdot : \mathbb{Z}^2 \to \mathbb{Z}$, $(x, y) \mapsto x \cdot y$ sînt operații binare pe $\mathbb{Z}$. Luarea opusului $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto -x$, este o operație unară, iar fixarea numărului 1984 este o operație nulară. În fine, funcția $f : \mathbb{Z}^3 \to \mathbb{Z}$, $f(x, y, z) = z \cdot (x + y)$ poate fi considerată o operație ternară pe $\mathbb{Z}$.

Semigrupuri, monoizi

Reamintim că un *semigrup* (*1/2-grup*) $(S, *)$ este o mulțime nevidă S împreună cu o operație binară $*$ pe S presupusă asociativă. Un 1/2-grup S având element neutru $e \in S$ se numește *monoid* și se mai notează $(S, *, e)$. Uneori un 1/2-grup $(S, *)$ sau un monoid $(S, *, e)$ este notat simplu cu S, reținînd doar mulțimea suport. Dacă $(S, *, e)$ este un monoid, atunci pentru orice $x, y \in S$ este definit elementul $x * y$ din S; în plus, $\forall\, x, y, z \in S$ avem

$$x * (y * z) = (x * y) * z \text{ și } x * e = e * x = x.$$

Are loc regula generală de asociativitate și aceasta permite să definim inductiv, pentru orice $x_1, \ldots, x_n \in S$, compusul $x_1 * x_2 * \ldots * x_n = x_1 * (x_2 * \ldots * x_n)$. Un monoid $(S, *, e)$ în care $\forall\, x, y \in S$, $x * y = y * x$ se numește *monoid comutativ*.

Exemple. 1) Pentru orice dinamică Peano $(N, s)_0$ se definesc două structuri — aditivă și multiplicativă de monoid, anume

$$(N, +, 0) \text{ și } (N, \cdot, 1).$$

Demonstrațiile necesare au fost date în § 1.2.

2) Pe mulțimea $M_n(\mathbb{R})$ a matricilor pătratice de ordin $n \geqslant 1$ cu coeficienți reali există o structură de monoid aditiv comutativ $(M_n(\mathbb{R}), +, 0)$ și o structură de monoid multiplicativ $(M_n(\mathbb{R}), \cdot, U_n)$ care nu este comutativ pentru $n \geqslant 2$.

Dacă $(S, *)$ este un 1/2-grup, $S' \subset S$ o mulțime și dacă $\forall\, x, y \in S'$, $x * y \in S'$, atunci se spune că S' este *sub* 1/2-*grup* al lui S și se mai scrie $S' \curvearrowright S$. Fie $(S, *, e)$ un monoid și $S' \subset S$. Dacă $\forall\, x, y \in S'$, $x * y \in S'$ și în plus $e \in S'$, atunci $(S', *, e)$ este numit *submonoid* al lui S și se scrie de asemenea $S' \curvearrowright S$.

Fie $(S, *)$, $(T, \circ)$ două 1/2-grupuri. Prin *morfism* de 1/2-grupuri de la $(S, *)$ la $(T, \circ)$ se înțelege orice aplicație de mulțimi $f : S \to T$ astfel încît $\forall\, x, y \in S$, $f(x * y) = f(x) \circ f(y)$, adică diagrama

$$\begin{array}{ccc} S \times S & \xrightarrow{\ *\ } & S \\ {\scriptstyle f \times f}\downarrow & & \downarrow{\scriptstyle f} \\ T \times T & \xrightarrow{\ \circ\ } & T \end{array}$$

să fie comutativă. Dacă $(S, *, e)$, $(T, \circ, e')$ sînt doi monoizi, orice aplicație $f : S \to T$ care este morfism de 1/2-grupuri și astfel încît $f(e) = e'$ se numește *morfism de monoizi*. Un morfism de monoizi $f : S \to T$ se numește *izomorfism*, dacă există un morfism $g : T \to S$ astfel încît $g \circ f = 1_S$ și $f \circ g = 1_T$. Se arată ușor că un morfism de monoizi $f : S \to T$ este un izomorfism, dacă și numai dacă f este aplicație bijectivă. Doi monoizi se spune că sînt *izomorfi* dacă între ei se poate stabili un izomorfism.

Exemple. 1) Dacă $(M, \cdot, e)$ este un monoid, atunci $(\mathfrak{p}(M), \cdot, \{e\})$ este de asemenea un monoid, punînd

$$\forall\, A, B \in \mathfrak{p}(M),\ A \cdot B = \{a \cdot b \mid a \in A, b \in B\}.$$

Aplicația $f : M \to \mathfrak{p}(M)$, $x \mapsto \{x\}$ este evident un morfism injectiv de monoizi.

2) Dacă X este o mulțime oarecare, atunci mulțimea Rel X a relațiilor binare pe X este un monoid relativ la compunere, $(\mathrm{Rel}\, X, *, 1_X)$, punînd $R * S = S \circ R$. Un submonoid al acestuia este mulțimea X^X a funcțiilor totale $X \to X$.

Fie $(S, *)$ un 1/2-grup și $\rho \subset S^2$ o relație binară pe S. Se spune că relația ρ este *compatibilă la stînga* (resp. *la dreapta*) cu operația $*$ dacă :

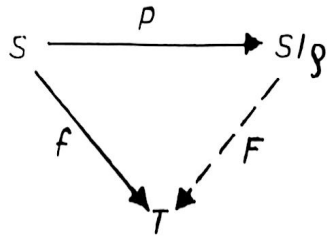
$$\forall\, x, x' \in S,\quad x \rho x' \Rightarrow (z * x) \rho (z * x') \quad [\text{resp. } (x * z) \rho (x' * z)],$$

pentru orice $z \in S$.

Dacă ρ este o relație de echivalență pe S, faptul că ρ este compatibilă cu $*$ (compatibilă la stînga și la dreapta) este echivalent cu aceea că

$$\forall\, x, x', y, y' \in S,\quad x \rho x' \text{ și } y \rho y' \Rightarrow (x * y) \rho (x' * y').$$

TEOREMA 1.6. *Fie* $(S, *)$ *un* 1/2-*grup și* ρ *o relație de echivalență pe* S *compatibilă cu* $*$. *Atunci mulțimea-cît* S/ρ *are o structură naturală de* 1/2-*grup și considerînd aplicația surjectivă* $p : S \to S/\rho$, $x \mapsto [x]$, *are loc următoarea proprietate de universalitate : pentru orice* 1/2-*grup* $(T, \circ)$ *și pentru orice morfism* $f : S \to T$ *de* 1/2-*grupuri, astfel încît* $\forall\, x, y \in S$, $x \rho y \Rightarrow f(x) = f(y)$, *există și este unic un morfism de* 1/2-*grupuri* $F : S/\rho \to T$ *pentru care* $F \circ p = f$, *adică este comutativă diagrama*



Demonstrație. Pentru orice $[x], [y] \in S/\rho$ $(x, y \in S)$ definim $[x] * [y] = [x * y]$; rezultatul operației depinde numai de clasele $[x], [y]$ și nu de reprezentanți ai acestora: dacă $[x'] = [x]$ și $[y'] = [y]$, atunci $x' \rho x$, $y' \rho y$, deci $(x' * y') \rho (x * y)$, adică $[x' * y'] = [x * y]$.

Operația algebrică $*$ astfel definită pe S/ρ este evident asociativă, iar aplicația $p : S \to S/\rho$, $x \mapsto [x]$ este un morfism (evident surjectiv) de semigrupuri. Pentru f dat ca în enunț se consideră aplicația

$$F : S/\rho \to T, \text{ definită prin } F([x]) = f(x).$$

Verificările necesare sînt imediate. ∎

Dacă S este un monoid (resp. un monoid comutativ), atunci aceeași proprietate o are S/ρ.

Grupuri

Reamintim că se numește *grup* orice monoid $(G, *, e)$ în care orice element admite un invers. Așadar, $\forall\, x \in G$, $\exists\, y \in G$ astfel încît $x * y = e$, $y * x = e$; acest y este unic (depinzînd de x), se numește inversul lui x și se notează x^{-1}. Un grup G este deci o mulțime pe care sînt definite :

— o operație binară $G \times G \to G$, $(x, y) \mapsto x * y$, presupusă asociativă ;

— o operație nulară de fixare a elementului neutru e ;

— o operație unară $G \to G$, $x \mapsto x^{-1}$ de luare a inversului.

Fie $(G, \cdot, e)$ un grup notat multiplicativ. Pentru orice element $a \in G$ se pot defini inductiv puterile a^n, $n \in \mathbb{N}$, prin $a^0 = e$, $a^1 = a$,

$a^n = a^{n-1} \cdot a$. Acest fapt are loc chiar și în orice monoid, dar într-un grup se pot defini și puterile întregi: $a^{-n} = (a^{-1})^n$, $n \geqslant 1$. Reamintim de asemenea că o submulțime $H \subset G$ astfel încît $\forall\, x, y \in H$, $xy^{-1} \in H$ se numește un *subgrup* al lui G (se scrie $H \leqslant G$). Grupurile comutative sînt numite de asemenea *grupuri abeliene* (N. H. Abel, 1802-1829).

Exemple. 1) Monoidul $(\mathbb{Z}, +, 0)$ este un grup abelian; se știe că subgrupurile sale sînt exact submulțimile de forma $k\mathbb{Z} = \{kx \mid x \in \mathbb{Z}\}$, $k \in \mathbb{N}$.

2) Fie o mulțime $M = \{a, b, c\}$ cu trei elemente. Există atunci șase aplicații bijective de la M la M și mulțimea lor formează un grup relativ la compunere, necomutativ.

Dacă $(G, *, e)$ și $(G', \circ, e')$ sînt două grupuri, reamintim că un morfism de la G la G' este o aplicație $f : G \to G'$ astfel încît

$$\forall\, x, y \in G,\ f(x * y) = f(x) \circ f(y).$$

În acest caz rezultă automat că $f(e) = e'$. Două exemple remarcabile de subgrupuri sînt: *nucleul lui* f, $\operatorname{Ker} f \leqslant G$, $\operatorname{Ker} f = \{x \in G \mid f(x) = e'\}$ și *imaginea lui* f, $\operatorname{Im} f \leqslant G'$, $\operatorname{Im} f = \{y \in G' \mid \exists\, x \in G, y = f(x)\} = f(G)$. Un morfism $f : G \to G'$ de grupuri se numește *izomorfism*, dacă există un morfism $g : G' \to G$ de grupuri astfel încît $g \circ f = 1_G$, $f \circ g = 1_{G'}$; o aplicație $f : G \to G'$ între două grupuri este un izomorfism dacă și numai dacă f este un morfism bijectiv.

Semiinele, inele

Se numește *semiinel* (1/2-*inel*) o mulțime A pe care sînt definite două operații binare — adunarea și înmulțirea și sînt fixate elemente $0 \in A$, $1 \in A$, avînd proprietățile următoare:

1) $(A, +, 0)$ este monoid comutativ;

2) $(A, \cdot, 1)$ este un monoid;

3) $\forall\, a, b, c \in A$, $a \cdot (b + c) = a \cdot b + a \cdot c$ și $(a + b) \cdot c = a \cdot c + b \cdot c$;

4) $\forall\, a \in A$, $a \cdot 0 = 0 \cdot a = 0$.

Vom nota uneori un astfel de semiinel prin $(A, +, \cdot, 0, 1)$; se scrie xy în loc de $x \cdot y$.

Un 1/2-inel în care orice $a \in A$ are un opus (notat $-a$) se numește *inel*. Dacă înmulțirea este comutativă, inelul se numește *comutativ*. Un inel în care orice element $a \in A \setminus \{0\}$ are invers relativ la înmulțire se numește *corp*.

Exemple. 1) $\mathbb{N}$ este un 1/2-inel; $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geqslant 0\}$ este de asemenea un 1/2-inel relativ la operațiile uzuale de adunare și înmulțire.

2) Codul binar $\mathbb{B} = \{0, 1\}$ este un corp relativ la operațiile $+$, $\cdot$ definite prin: $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, $1 + 1 = 0$; $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$; apoi $\mathbb{B}$ este semiinel relativ la operațiile $\vee$, $\wedge$ definite prin $0 \vee 0 = 0$, $0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1$; $0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0$, $1 \wedge 1 = 1$.

3) Un inel A se numește *boolean* dacă $\forall\, a \in A,\ a^2 = a$. În acest caz, $\forall\, a \in A$ avem $2a = 0$, deci $-a = a$ [deoarece $\forall\, a \in A$ avem $(a + a)^2 = a + b$, adică $(2a)^2 = 2a$, $4a^2 = 2a$; cum $a^2 = a$, rezultă $2a = 0$], Apoi $\forall\, a,\ b \in A$, avem $a + b = (a + b)^2 = a^2 + + ab + ba + b^2 = a + ab + ba + b$, deci $ab + ba = 0$, deci $ab = -ba = ba$. Prin urmare orice inel boolean este comutativ. Inelul $\mathbb{B}$ este boolean; de asemenea, $\mathfrak{p}(M)$ este un inel boolean relativ la diferența simetrică $(+)$ și intersecție $(\cdot)$.

Dacă A, B sînt două 1/2-inele, se numește *morfism de 1/2-inele de la A la B* orice aplicație $f : A \to B$ astfel încît $\forall\, x, y \in A$, $f(x + y) = = f(x) + f(y)$, $f(xy) = f(x)f(y)$, $f(0)$ 0 și $f(1) = 1$.

§ 1.4. DICȚIONARUL UNUI ALFABET; DINAMICI PESTE O MULȚIME OARECARE

Litere, cuvinte

Să considerăm o mulțime nevidă X numită ad-hoc *alfabet* și ale cărei elemente se vor numi *litere*. X poate fi o mulțime de simboluri sau de caractere, a căror natură nu este precizată.

Orice șir finit de elemente (litere) din X se numește *cuvînt* în X. Mai precis, un cuvînt de lungime $n (n \geqslant 1)$ este o funcție

$$c : S_n \to X, \quad \text{unde } S_n = \{x \in \mathbb{N} \mid x < n\}.$$

Notînd $c_k = c(k)$, $\forall\, k \in S_n$, se mai scrie $c = c_0 c_1 \ldots c_{n-1}$. Pentru $n = 0$ există prin convenție un singur cuvînt de lungime zero, numit *cuvîntul vid* și notat $\wedge$ (sau $\wedge_X$). Mulțimea cuvintelor de lungime n în alfabetul X se identifică prin X^n, oricare ar fi $n \in \mathbb{N}$. Cuvintele apar deci ca secvențe de litere. Vom prezenta mai tîrziu un nou procedeu de inducție, de exemplu peste lungimea cuvintelor.

Două cuvinte nevide $c = a_1 a_2 \ldots a_p$, $d = b_1 b_2 \ldots b_q$ în X sînt egale, dacă și numai dacă au aceeași lungime (adică $p = q$) și coincid literă cu literă ($a_1 = b_1, \ldots, a_p = b_p$). Un cuvînt nevid în X nu poate fi egal cu $\wedge_X$.

DEFINIȚIA 1.10. Se notează cu X^* mulțimea tuturor cuvintelor în X, numită *dicționarul (sintactic) al alfabetului* X. Așadar,

$$X^* = \bigcup_{n \geqslant 0} X^n \text{ (uneori se notează } X^+ = \bigcup_{n \geqslant 1} X^n = X^* \setminus \{\wedge_X\}).$$

Pe mulțimea X^* pot fi introduse mai multe relații binare; pentru $c_1, c_2 \in X^*$ punem

$c_1 < c_2 \leftrightarrow l(c_1) \leqslant l(c_2)$ [$l(c)$ este lungimea cuvîntului c];

$c_1 \subset c_2 \leftrightarrow \exists\, u, v \in X^*$ astfel încît $c_2 = u c_1 v$ [se spune atunci:

c_1 este subcuvînt al lui c_2 sau c_1 intră în c_2];

$$c_1 \sim c_2 \leftrightarrow l(c_1) = l(c_2).$$

„$<$" este relație de preordine, „$\subset$" relație de ordine iar „$\sim$" de echivalență.

Limbaje

Orice submulțime $L \subset X^*$ se numește *limbaj* în (sau peste) alfabetul X. Un limbaj într-un alfabet este prin urmare o colecție de cuvinte în acel alfabet. Mulțimea limbajelor în alfabetul X este tocmai $\mathbf{p}(X^*)$.

Exemple. 1) Fie $X = \mathbb{B} = \{0, 1\}$ codul binar. Atunci 11010, 01000 sînt cuvinte binare (în $\mathbb{B}$) de lungime 5. În general cuvintele binare nevide apar ca șiruri finite de 0 și 1 și de aceea se mai numesc secvențe de biți. Mulțimea lor se notează cu $\mathbb{B}^*$.

2) Fie $X = \mathbb{1} = \{|\}$; atunci $X^* = \{\wedge, |, ||, |||, \ldots\}$. Notînd $|^n = \underbrace{|| \ldots |}_{n \text{ ori}}$, $n \geqslant 1$, se poate considera bijecția $f : \mathbb{N} \setminus \{0\} \to \mathbb{1}^+ = X^* \setminus \{\wedge\}$, $n \mapsto |^n$ și $\mathbb{N}$ se identifică prin $\mathbb{1}^*$.

Să remarcăm de asemenea că notînd $K = \{0, 1, 2, \ldots, 9\}$, mulțimea cifrelor zecimale, atunci $N_K = K^+ = K^* \setminus \{\wedge_K\}$; așa cum am văzut la p. 32, elementele lui N_K sînt tocmai numerele naturale (în scrierea zecimală). Așadar, aceeași mulțime de elemente poate fi descrisă ca limbaj în alfabete distincte.

3) Fie $X = \{a, b, c, \ldots, x, y, z\}$ alfabetul limbii române (litere mici). Cuvintele „studiu", „timp", „aab" etc. aparțin dicționarului sintactic X care este mai bogat decît dicționarul semantic al limbii române (acesta cuprinde cuvintele cărora li se atribuie un înțeles).

4) Programele scrise într-un limbaj de programare reprezintă un exemplu de limbaj peste o anumită mulțime de caractere.

5) Fie X un alfabet. Dacă u și v sînt două cuvinte în X, se notează cu uv cuvîntul obținut prin juxtapunerea literelor lui u și v, numit *concatenatul* lui u și v. Dacă L și L' sînt două limbaje în X, atunci se pot considera noi limbaje: *reuniunea* $L \cup L'$, *concatenatul* $L \cdot L' = \{cd \mid c \in L, d \in L'\}$, *iteratul* $L^* = \bigcup_{n \geqslant 0} L^n$, unde $L^0 = \{\wedge\}$ și $L^n = \{c_1 \ldots c_n \mid$ toți $c_i \in L\}$ este mulțimea tuturor cuvintelor obținute prin concatenarea a cîte n cuvinte din limbajul L (iterarea se mai numește și „operația star" a lui Kleene).

Mulțimea $\mathbf{p}(X^*)$ *a tuturor limbajelor în alfabetul* X *este un semiinel în general necomutativ, relativ la operațiile de reuniune* $(+)$ *și concatenare* $(\cdot)$. Într-adevăr, $(\mathbf{p}(X^*), \cup, \emptyset)$ este un monoid comutativ; $(\mathbf{p}(X^*), \cdot, \wedge)$ este un monoid; apoi $\forall L, L', L'' \in \mathbf{p}(X^*)$, $L \cdot (L' \cup L'') = (L \cdot L') \cup (L \cdot L'')$, $(L' \cup L'') \cdot L = (L' \cdot L) \cup (L'' \cdot L)$ și $L \cdot \emptyset = \emptyset \cdot L = \emptyset$.

DEFINIȚIA 1.11. Fie X un alfabet fixat și M o mulțime oarecare. Se numește *codificare a lui* M *în alfabetul* X, orice aplicație

$$\gamma : M \to \mathbf{p}(X^*)$$

astfel încît $\forall u, v \in M$, $u \neq v$ să avem $\gamma(u) \cap \gamma(v) \quad \emptyset$.

Așadar, oricărui element $u \in M$ i se asociază un limbaj $\gamma(u) \subset$ $\subset X^*$, care descrie în X acel element și la elemente distincte din M corespund limbaje disjuncte.

Dacă A și B sînt două alfabete, se numește *traducere în* B a unui limbaj $L \subset A^*$ orice aplicație injectivă

$$\tau : L \to B^*.$$

Notînd $L_1 = \tau(L) \subset B^*$, este definită o aplicație bijectivă $L \to L_1$, $x \mapsto \tau(x)$, a cărei inversă permite recuperarea lui L.

Aplicație

Un *translator* $\mathbf{T} = (L', L'', t, L)$ este un 4-uplu în care L' este limbajul de intrare (sursă), L'' limbajul de ieșire, $t : L' \to L''$ este o funcție parțială (traducere), iar L este limbajul propriu al translatorului, în care este programat. Se scrie pe scurt: $\mathbf{T} = (L' \xrightarrow[L]{t} L'')$.

Există două operații între translatoare, nu peste tot definite:

— *compunerea*: $(L' \xrightarrow[L]{t'} L'') \circ (L'' \xrightarrow[L]{t''} L''') = (L' \xrightarrow[L]{t'' \circ t'} L''')$

— *codificarea*: $(L_1 \xrightarrow[L]{t_1} L_2) * (L' \xrightarrow[L_1]{t} L'') = (L' \xrightarrow[L_2]{t} L'')$.

Așadar, dacă translatorul $(L' \xrightarrow[L_1]{t} L'')$ este programat tocmai în limbajul de intrare al translatorului $(L_1 \xrightarrow[L]{t_1} L_2)$, atunci prin codificare se obține reprezentarea primului translator în limbajul de ieșire al celui de al doilea.

Fie L_1 limbajul unei mașini M_1 și L_2 limbajul unei mașini M_2. Presupunem că pe mașina M_1 translatorul $(L \xrightarrow[L_1]{t} L_1)$ realizează traducerea dintr-un limbaj superior L_1 al mașinii, iar translatorul $(L \xrightarrow[L]{t'} L_2)$ realizează traducerea din L în L_2, fiind programat în limbajul L. Atunci aplicînd operația de codificare se poate obține un translator din L în limbajul L_2 al mașinii M_2. Anume, $(L \xrightarrow[L_1]{t} L_1) * (L \xrightarrow[L]{t'} L_2) = (L \xrightarrow[L_1]{t'} L_2)$; $(L \xrightarrow[L_1]{t'} L_2) * (L \xrightarrow[L]{t'} L_2) = (L \xrightarrow[L_2]{t'} L_2)$.

Așadar, *se recomandă scrierea unui program într-un limbaj superior cu codificare ulterioară în limbajul mașinii de lucru.*

Să notăm acum cu L_0 limbajul unei anumite mașini M și să presupunem că avem translatoare $(L_2 \xrightarrow[L_2]{} L_2), (L_2 \xrightarrow[L_1]{} L_1), (L_1 \xrightarrow[L_0]{} L_0)$ din limbaje ordonate prin relația de superioritate. Atunci prin operații de codificare și compunere, pentru orice pereche de limbaje (L_i, L_j), $0 \leqslant j < i \leqslant 3$, se poate obține un translator pentru mașina M care realizează traducerea din limbajul (superior) L_i în limbajul L_j. Anume, pentru a obține un translator $(L_2 \xrightarrow[L_0]{} L_0)$ este suficient să realizăm codificarea $(L_1 \xrightarrow[L_0]{} L_0) * (L_2 \xrightarrow[L_1]{} L_1) = (L_2 \xrightarrow[L_0]{} L_1)$.

Apoi, prin compunere, avem $(L_2 \xrightarrow[L_0]{} L_1) \circ (L_1 \xrightarrow[L_0]{} L_0) = (L_2 \xrightarrow[L_0]{} L_0)$. În mod analog, $(L_2 \xrightarrow[L_0]{} L_0) * (L_3 \xrightarrow[L_3]{} L_2) = (L_3 \xrightarrow[L_0]{} L_2)$ și $(L_3 \xrightarrow[L_6]{} L_2) \circ (L_2 \xrightarrow[L_0]{} L_0) = (L_3 \xrightarrow[L_6]{} L_0)$. Așadar, *construirea unui translator dintr-un limbaj superior de programare constă în evidențierea ierarhiei unor limbaje de nivel intermediar, în realizarea traducerilor adiacente și în conjugarea globală a acestora.*

În mod similar pot fi introduse în discuție *interpretoarele*. Noțiunile de matematică discretă introduse pînă acum, ca și cele de graf, arbore, algebră universală, model etc., permit, printre altele, formalizarea proceselor de programare și studiul esenței structurale a acestora ([18], [28], [31], [35], [44], [54], [58]).

Monoidul liber generat de un alfabet

Fie X o mulțime oarecare (alfabet). Pe dicționarul X^* se poate considera o operație algebrică specifică deosebit de importantă, anume concatenarea (sau juxtapunerea) cuvintelor, pe care am descris-o anterior.

Fie $c \in X^*$, $c = c_1 \ldots c_n$, un cuvînt de lungime n ($n \geqslant 1$) și $d \in X^*$, $d = d_1, \ldots, d_m$ un cuvînt de lungime m ($m \geqslant 1$). Atunci se poate considera cuvîntul de lungime $n + m$ definit astfel:

$$u: \; S_{n+m} \to X, \quad u(i) = \begin{cases} c_i & \text{dacă } 1 \leqslant i \leqslant n, \\ d_{i-n} & \text{dacă } n+1 \leqslant i \leqslant n+m, \end{cases}$$

numit *concatenatul lui c și d* și notat $u = j(c, d)$.

Așadar,

$$j(c_1 \ldots c_n, d_1 \ldots d_m) = c_1 \ldots c_n d_1 \ldots d_m.$$

De asemenea, pentru orice $c \in X^*$ se pune, prin definiție,

$$j(\wedge, c) = c, \quad j(c, \wedge) = c.$$

Operația binară

$$j: X^* \times X^* \to X^*$$

astfel definită se numește *concatenarea* (sau *juxtapunerea*) cuvintelor în X. Uneori se scrie pentru comoditate cd în loc de $j(c, d)$, pentru orice $c, d \in X^*$.

Este evident că operația de concatenare este asociativă și cuvîntul vid $\wedge = \wedge_X$ este un element neutru. Așadar, pe dicționarul X^* este definită o structură de monoid $(X, j, \wedge_X)$, numit *monoidul liber generat de alfabetul X*. Acest monoid este în general necomutativ. El constituie un obiect fundamental de studiu în teoria limbajelor formale.

Orice cuvînt din X^* este obținut prin concatenarea literelor sale. Pentru orice $a \in X$ vom nota

$$a^n = j(\overbrace{a, \ldots, a}^{n \text{ ori}}), \qquad n \geqslant 1 \text{ și } a^0 = \wedge .$$

Exemplu. Dacă $X = \mathbb{B}$, atunci cuvîntul binar 111 se scrie 1^3, iar cuvîntul 1111010011 se poate scrie $1^4010^21^2$.

Observație. Operația de concatenare poate fi introdusă și ca un exemplu de definiție dată prin inducție. Anume, X fiind o mulțime fixată, se definesc X^* și funcția lungime $l : X^* \to \mathbb{N}$ astfel:

1) X^* conține un element distins, cuvîntul vid $\wedge$ și punem $l(\wedge) = 0$ (baza inducției);

2) dacă $c \in X^*$ și $x \in X$, atunci $xc \in X^*$ și $l(xc) = l(c) + 1$ (pasul de inducție). Definim apoi aplicația de concatenare $j : X^* \times X^* \to X^*$, $(c, d) \mapsto cd$ prin inducție după lungimea lui c astfel:

1) $j(\wedge, d) = d$ (baza inducției);

2) $j(xc, d) = j(x, cd)$ (pasul de inducție).

Se verifică imediat că $l(cd) = l(c) + l(d)$ (asociativitatea concatenării) și că $\forall\, c \in X^*$, $c \wedge = \wedge c = c$.

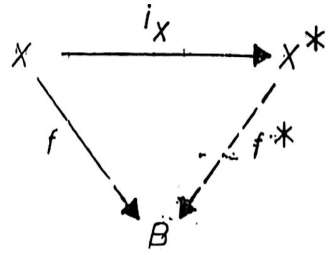
Proprietatea de universalitate

Fie X o mulțime nevidă. Vom nota cu

$$i_X : X \to X^*, \quad a \mapsto a,$$

aplicația injectivă canonică, prin care fiecărei litere $a \in X$ i se asociază cuvîntul a. Atunci are loc următoarea proprietate a lui X^* care exprimă comportarea sa față de orice alt monoid, indicînd că într-un anumit sens X^* este monoidul „cel mai apropiat" de X.

TEOREMA 1.7. *Fie X un alfabet, $(X^*, j, \wedge)$ monoidul liber generat de X. Pentru orice monoid $(B, \circ, e)$ și pentru orice aplicație de mulțimi $f : X \to B$, există și este unic un morfism de monoizi $f^* : X^* \to B$ astfel încît $f^* \circ i_X = f$, adică diagrama*



să fie comutativă.

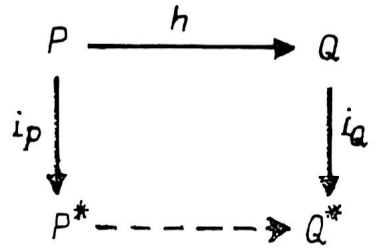
Demonstrație. Pentru orice cuvînt $c = a_1 \ldots a_k \in X^*$, $k \geqslant 1$, definim $f^*(c) = f(a_1) \circ \ldots \circ f(a_k)$; de asemenea, punem $f^*(\wedge) = e$. În particular, $\forall\, a \in X$, avem $f^*(a) = a$. Aplicația $f^* : X^* \to B$ astfel definită este un morfism de monoizi deoarece

$$\forall\, c, d \in X^*,\ f^*(j(c, d)) = f(c) \circ f(d) \quad \text{și} \quad f^*(\wedge) = e.$$

În plus, $\forall\, a \in X$, $(f^* \circ i_X)(a) = f^*(i_X(a)) = f^*(a) = f(a)$, deci $f^* \circ i_X = f$.

Rămîne să dovedim unicitatea morfismului f^* (avînd proprietatea $f^* \circ i_X = f$). Fie $g : X^* \to B$ un alt morfism de monoizi, astfel încît $g \circ i_X = f$. Atunci $g \circ i_X = f^* \circ i_X$, deci $\forall\, a \in X$, $g(a) = f^*(a) = f(a)$ și ca atare, $\forall\, c = a_1 \ldots a_k \in X^*$ avem $c = j(a_1, \ldots, a_k)$, deci $g(c) = g(j(a_1, \ldots, a_k)) = g(a_1) \circ \ldots \circ g(a_k) = f(a_1) \circ \ldots \circ f(a_k) = f^*(c)$. Așadar, $g = f^*$ pe X^*. ∎

COROLAR. *Dacă P și Q sînt două alfabete și $h : P \to Q$ este o aplicație oarecare de mulțimi, atunci există și este unic un morfism de monoizi $h^* : P^* \to Q^*$ făcînd comutativă diagrama*



Vom da în cele ce urmează o caracterizare intrinsecă a monoidului liber X^* generat de o mulțime X, extinzînd caracterizarea dată de Peano pentru $\mathbb{N}$. Aceasta din urmă se regăsește luînd $X = \mathbb{1}$.

Monoizi liberi

DEFINIȚIA 1.12. Fixăm o mulțime nevidă X, numită în continuare alfabet. Vom numi *monoid liber generat de* X un monoid D împreună cu o aplicație $i : X \to D$ cu proprietatea că oricare ar fi un monoid M și o aplicație de mulțimi $f : X \to M$, există și este unic un morfism de monoizi $f^* : D \to M$ astfel încît $f^* \circ i = f$.

Am construit mai înainte un monoid liber generat de X, anume dicționarul X^* al alfabetului X, cu structura de monoid definită de concatenare și de cuvîntul vid $\wedge_X$; de asemenea, am construit aplicația $i_X : X \to X^*$, $x \mapsto x$ (identificînd litera x cu cuvîntul format numai din litera x). Dacă $X = \mathbb{1} = \{\lambda\}$, atunci dicționarul X^* constă din cuvinte de forma

$$\wedge, \lambda, \lambda\lambda, \lambda\lambda\lambda, \ldots,$$

care pot fi identificate cu numerele naturale 0, 1, 2, 3, . . . , deci $X^* = \mathbb{N}$. Putem însă arăta și direct că $(\mathbb{N}, +, 0)$ împreună cu aplicația $i : \mathbb{1} \to \mathbb{N}$, $\lambda \mapsto 1$, este un monoid liber generat de $\mathbb{1}$. [Într-adevăr, fie $(M, \cdot, e)$ un alt monoid și $f : \mathbb{1} \to M$, $\lambda \mapsto a$ o aplicație oarecare. Organizăm pe M ca o dinamică cu inițializare, considerînd aplicația $h : M \to M$, $x \mapsto xa$ și elementul $a \in M$. Conform teoremei 1.1 de inițialitate există și este unic un morfism de dinamici

$$f^* : (\mathbb{N}, s)_0 \to (M, h)_e \text{ astfel încît } f^*(0) = e;$$

așadar, $f^* \circ s = h \circ f^*$. Avem $f^*(1) = f^*(s(0)) = (f^* \circ s)(0) = h(f^*(0)) = h(e) = ea = a$, deci $f^* \circ i = f$. Prin inducție după n, se arată imediat că $f^*(m + n) = f^*(m) \cdot f^*(n)$, deci $f^* : \mathbb{N} \to M$ este un morfism de monoizi. În fine, unicitatea lui f^* rezultă din faptul că orice morfism de monoizi $g : \mathbb{N} \to M$ cu proprietatea că $g \circ i = f$ (adică $g(1) = a$) satisface $g(0) = e$ și $\forall\, n \in \mathbb{N}$, $g(s(n)) = g(n + 1) = g(n) \cdot g(1) = g(n) \cdot a = h(g(n))$, deci g este și el un morfism de dinamici cu inițializare închizînd aceeași diagramă ca și f^*, deci $g = f^*$.]

Așa cum am spus, vom da în cele ce urmează o caracterizare intrinsecă a conceptului de monoid liber generat de X. Mai întîi să observăm că dacă D_1 și $i_1 : X \to D_1$, D_2 și $i_2 : X \to D_2$ sînt doi monoizi liber generați de X, atunci există un izomorfism de monoizi $u : D_1 \to D_2$ astfel încît $u \circ i_1 = i_2$ (și $u^{-1} \circ i_2 = i_1$). Prin urmare, sursa de inspirație în degajarea proprietăților interne ale monoizilor liber generați de X poate fi oricare dintre aceștia și, desigur, vom utiliza pe cel pe care îl cunoaștem cel mai bine, anume dicționarul alfabetului X. Vom lua precauția ca în continuare toate rezultatele care au ca obiect echivalența diverselor definiții pentru conceptul de monoid liber generat să nu depindă de existența vreunui exemplu concret de monoid liber generat. Deoarece $\mathbb{N}$ este un monoid liber generat de $\mathbb{1}$, iar X^* se poate construi folosind $\mathbb{N}$, pentru a fi consecvenți vom separa rezultatele care utilizează numere naturale de cele care nu utilizează $\mathbb{N}$.

Rezultatele care urmează au de asemenea scopul de a convinge cititorul asupra forței proprietății de universalitate care definește conceptul de monoid liber generat.

LEMA 4. *Dacă D, $i : X \to D$, este un monoid liber generat de alfabetul X, atunci orice submonoid al lui D care include $i(X)$ coincide cu D, adică $\overline{i(X)} = D$* (Pentru o submulțime $B \subset D$ am notat cu $\bar{B}$ submonoidul lui D generat de B, deci cel mai mic submonoid al lui D care include pe B).

Demonstrație. Fie $f : X \to \overline{i(X)}$, $x \mapsto i(x)$ și $\bar{f} : D \to \overline{i(X)}$ unicul morfism de monoizi astfel încît $\bar{f} \circ i = f$. Să notăm cu $j : \overline{i(X)} \to D$ morfismul de incluziune. Deoarece $j \circ \bar{f}$ este morfism și, în plus, $(j \circ \bar{f}) \circ i = j \circ (\bar{f} \circ i) = j \circ f = i$, rezultă că $j \circ \bar{f} = 1_D$. De aici rezultă că aplicația j este surjectivă deci $\overline{i(X)} = D$. ∎

Această lemă stă la baza unui caz special de inducție pe care o vom numi *inducție monoidală pe* D :

Fie $\mathbf{p} : D \to \mathbb{B} = \{\mathbf{F}, \mathbf{A}\}$ un predicat astfel încît :

1) $\mathbf{p}(i(x)) = \mathbf{A}$, pentru orice $x \in X$ (*baza de inducție*) ;

2) $\mathbf{p}(e) = \mathbf{A}$, unde e este elementul neutru al lui D și ori de cîte ori $u, v \in D$ și $\mathbf{p}(u) = \mathbf{A}$, $\mathbf{p}(v) = \mathbf{A}$, rezultă că $\mathbf{p}(uv) = \mathbf{A}$ (*pasul de inducție*). Atunci $\mathbf{p}$ este adevărat pe orice element din D.

Într-adevăr, notînd $D' = \{u \in D \mid \mathbf{p}(u) = \mathbf{A}\}$, rezultă că D' este un submonoid al lui D care conține $i(X)$ și conform lemei 4, rezultă că $D' = D$, ceea ce trebuia dovedit.

Dacă monoidul D împreună cu aplicația $i : X \to D$ este liber generat de X, atunci elementele lui D nu sînt neapărat cuvintele dicționarului lui X ; totuși ele au „lungime" și sînt „alcătuite din litere". Anume, să considerăm monoidul $(\mathbb{N}, +, 0)$ și fie $f : X \to \mathbb{N}$, $x \mapsto 1$. Vom nota cu

$$l : D \to \mathbb{N}$$

unicul morfism de monoizi astfel încît $l \circ i = f$. Au loc proprietățile următoare :

1) $l(i(x)) = 1, \quad \forall\, x \in X$;

2) $l(e) = 0$;

3) $l(uv) = l(u) + l(v), \quad \forall\, u, v \in D$;

De asemenea, prin inducție monoidală se probează imediat că :

4) $u \in D, l(u) = 1 \leftrightarrow u \in i(X)$;

5) $u \in D, l(u) = 0 \leftrightarrow u = e$.

Considerăm apoi monoidul $(\mathbf{p}(X), \cup, \emptyset)$ și funcția $g : X \to \mathbf{p}(X)$, $x \mapsto \{x\}$. Vom nota cu

$$L : D \to \mathbf{p}(X)$$

unicul morfism de monoizi astfel încît $L \circ i = g$. Au loc proprietățile :

1′) $L(i(x)) = x$ pentru orice $x \in X$;

2′) $L(e) = \emptyset$;

3') $L(uv) = L(u) \cup L(v)$, $\forall\, u, v \in D$;

Prin inducție monoidală se arată că

4') $\forall\, u \in D$, $|L(u)| \leqslant l(u)$

și, în particular, $\forall\, u \in D$ mulțimea $L(u)$ este finită.

În același spirit se poate defini o funcție $\nu : D \to \mathbb{N}^X$ astfel încît $\forall\, u \in D$, $\forall\, x \in X$, $\nu(u)(x) =$ „numărul de apariții ale lui x în u".

X-dinamici Peano

În vederea studiului intrinsec al dicționarului unui alfabet vom utiliza o generalizare a conceptului de dinamică, studiat în § 1.2.

Fixăm un alfabet X nevid.

DEFINIȚIA 1.13. Vom numi *X-dinamică* orice pereche (A, δ) formată dintr-o mulțime A și o aplicație

$$\delta : A \times X \to A.$$

Un morfism de X-dinamici

$$f : (A_1, \delta_1) \to (A_2, \delta_2)$$

este o aplicație $f : A_1 \to A_2$ astfel încît $\forall\, a \in A_1$, $x \in X$, $f(\delta_1(a, x)) = \delta_2(f(a), x)$, ceea ce revine la comutativitatea diagramei

$$\begin{array}{ccc} A_1 \times X & \xrightarrow{f \times 1_X} & A_2 \times X \\ \downarrow{\scriptstyle \delta_1} & & \downarrow{\scriptstyle \delta_2} \\ A_1 & \xrightarrow{f} & A_2 \end{array}$$

Exemple. 1) Fie $(A, \cdot, e)$ un monoid și $X \subset A$ o submulțime. Definim aplicația $\delta : A \times X \to A$, $(a, x) \mapsto ax$. Atunci (A, δ) este o X-dinamică care va juca un rol important; în particular, pentru monoidul $A = X^*$ relativ la juxtapunerea cuvintelor, avem X-dinamica $\delta : X^* \times X \to X^*$, $(w, x) \mapsto wx$ obținută prin „adăugarea cîte unei litere la dreapta".

2) Dacă (A, δ) este o X-dinamică, atunci $A \times X$ are o structură de X-dinamică dată de aplicația $\delta \times 1_X : (A \times X) \times X \to A \times X$. În plus, aplicația δ definește un morfism de dinamici $(A \times X, \delta \times 1_X) \to (A, \delta)$.

Interpretare sistemică

Dacă (A, δ) este o X-dinamică, putem interpreta X ca mulțimea intrărilor și A ca mulțimea stărilor unui sistem, iar $\delta : A \times X \to X$, $(a, x) \mapsto \delta(a, x)$ ca aplicație de tranziție a stărilor, asociind

oricărei stări $a \in A$ și oricărei intrări $x \in X$ starea $\delta(a, x)$. Se poate considera de asemenea familia de aplicații $\{\delta_a\}_{a \in A}$, $\delta_a : X \to X$, $x \mapsto \delta(a, x)$.

Dacă fixăm o stare inițială $i \in A$ și o mulțime de stări terminale $T \subset A$ se obține un X-automat deterministic în sensul lui Eilenberg.

O *X-subdinamică* a unei dinamici (A, δ) este orice parte $S \subset A$ astfel încît $\delta(S \times X) \subset S$. Incluziunea canonică $i : S \to A$, $x \mapsto x$, este atunci un morfism de dinamici. Subdinamica *generată* de o parte $M \subset A$ este intersecția tuturor subdinamicilor care includ pe M și se notează $\overline{M}$; dacă $a \in A$, atunci în loc de $\overline{\{a\}}$ vom nota simplu $\bar{a}$.

Dacă $X = \mathbf{1}$ și $A \times X$ se identifică cu A, atunci dinamicile (în sensul definiției 1.5) coincid cu X-dinamicile.

DEFINIȚIA 1.14. Vom numi *X-dinamică Peano* orice triplet $(D, \delta)_d$ unde (D, δ) este o X-dinamică și $d \in D$ astfel încît să fie verificate următoarele proprietăți :

P1. $d \notin \delta(D \times X)$;

P2. δ este injectivă;

P3. orice X-subdinamică a lui D care conține d coincide cu D (sau, echivalent, $\bar{d} = D$).

Proprietatea P3 stă la baza unui tip nou de inducție pe D pe care o vom numi *inducție succesivă* :

Dacă $\mathbf{p} : D \to \mathbb{B} = \{\mathbf{F}, \mathbf{A}\}$ este un predicat astfel încît :

1) $\mathbf{p}(d) = \mathbf{A}$ (baza inducției);

2) $\forall x \in X, \{u \in D, \mathbf{p}(u) = \mathbf{A} \Rightarrow \mathbf{p}(\delta(u, x)) = \mathbf{A}\}$,

atunci pentru orice $u \in D$, $\mathbf{p}(u) = \mathbf{A}$ (pasul de inducție).

Într-adevăr, notînd $D' = \{u \in D \mid \mathbf{p}(u) = \mathbf{A}\}$, atunci D' este o X-subdinamică a lui D care conține d, deci $D' = D$, conform P3.

Ca și în cazul dinamicilor Peano vom demonstra o proprietate de universalitate care caracterizează X-dinamicile Peano și permite definițiile prin recurență (mai bine spus, X-recurență într-un sens care va fi precizat).

TEOREMA 1.8. *Fie (D, δ) o X-dinamică și un element $d \in D$. Afirmațiile următoare sînt echivalente :*

(i) *$(D, \delta)_d$ este o X-dinamică Peano;*

(ii) *Oricare ar fi X-dinamica (A, δ_1) și elementul $\alpha \in A$, există și este unic un morfism de X-dinamici $h : (D, \delta) \to (A, \delta_1)$ astfel încît $h(d) = \alpha$.*

Demonstrație. Implicația (i) $\Rightarrow$ (ii) exprimă o proprietate de inițialitate a X-dinamicilor Peano. Demonstrația dată mai jos acestei

implicații extinde pe cea a teoremei 1.1 și de aceea ne vom limita la a puncta etapele esențiale. Considerăm mulțimea de relații

$$\mathfrak{R} = \{\rho \subset D \times A \mid (d, \alpha) \in \rho \text{ și dacă } (u, a) \in \rho, \text{ atunci } \forall x \in X,$$

$$(\delta(u, x), \delta_1(a, x)) \in \rho\}.$$

Evident, $D \times A \in \mathfrak{R}$ și notăm $h = \bigcap_{\rho \in \mathfrak{R}} \rho$. Se arată, folosind inducția succesivă, că $\forall u \in D$ mulțimea $\{a \in A \mid (u, a) \in h\}$ are exact un element. De aici rezultă că h este o funcție, un morfism de X-dinamici și, în plus, $h(d) = \alpha$. Unicitatea lui h se arată probînd prin inducție succesivă că pentru orice alt morfism de X-dinamici $f : (D, \delta) \to (A, \delta_1)$ astfel încît $f(d) = \alpha$ avem $\forall u \in D$, $f(u) = h(u)$.

Demonstrăm acum implicația (ii) $\Rightarrow$ (i). Mai întîi arătăm că (ii) $\Rightarrow$ P1. Să considerăm X-dinamica $\mathbb{B} = \{0, 1\}$ definită prin

$$\delta' : \mathbb{B} \times X \to \mathbb{B}, \quad (b, x) \mapsto 1.$$

Conform ipotezei, există un morfism de X-dinamici

$$h : D \to \mathbb{B} \text{ astfel încît } h(d) = 0.$$

Dacă am avea $d \in \delta(D \times X)$, atunci $d = \delta(u, x)$ cu $u \in D$, $x \in X$, deci, h fiind un morfism de X-dinamici, $h(d) = \delta'(h(u), x) = 1$ și s-ar ajunge la o contradicție.

(ii) $\Rightarrow P_3$. Demonstrația este similară cu cea a lemei 4 și o omitem. Datorită lui P_3 vom putea folosi în continuare inducția succesivă pe D.

(ii) $\Rightarrow P_2$. Vom demonstra mai întîi un rezultat auxiliar. Reamintim că $D \times X$ are o structură de X-dinamică dată de $\delta \times 1_X$. Să arătăm că dacă (A, δ_1) este o X-dinamică, atunci orice două morfisme de X-dinamici

$$f, f' : (D \times X, \delta \times 1_X) \to (A, \delta_1)$$

care coincid pe $\{d\} \times X$, coincid peste tot. Anume, vom arăta prin inducție succesivă după u că

$$(*) \qquad f(u, x) = f'(u, x) \quad \textit{pentru orice } x \in X.$$

Pentru $u = d$ afirmația (*) este adevărată prin ipoteză. Fie apoi $u \in D$ un element pentru care afirmația este adevărată. Atunci $\forall\, y \in X$, $\forall\, x \in X$, $f(\delta(u, y), x) = \delta_1(f(u, y), x) = \delta_1(f'(u, y), x) = f'(\delta(u, y), x)$. Astfel afirmația (*) este demonstrată.

Vom adjuncționa la $D \times X$ un element $\beta \notin D \times X$ considerînd $D' = (D \times X) \cup \{\beta\}$. Definim aplicația

$$\delta' : D' \times X \to D', \quad \delta'(t, x) = \begin{cases} (\delta(t), x) & \text{dacă } t \in D \times X, \\ (d, x) & \text{dacă } t = \beta. \end{cases}$$

Se verifică imediat că incluziunea canonică $j : D \times X \to D'$ este un morfism de X-dinamici, adică diagrama

$$\begin{array}{ccc} (D \times X) \times X & \xrightarrow{j \times 1_X} & D' \times X \\ \downarrow{\scriptstyle \delta' \times 1_X} & & \downarrow{\scriptstyle \delta'} \\ D \times X & \xrightarrow{j} & D' \end{array}$$

este comutativă. Conform ipotezei (ii) va exista un morfism de X-dinamici

$$h : D \to D' \quad \text{astfel ca } h(d) = \beta.$$

Dar atunci $h \circ \delta : D \times X \to D'$ este și el un morfism de X-dinamici și $\forall\, x \in X$, $(h \circ \delta)(d, x) = h(\delta(d, x)) = \delta'(h(d), x) = \delta'(\beta, x) = (d, x) = j(d, x)$. Așadar, morfismele de X-dinamici $h \circ \delta$ și j coincid pe $\{d\} \times X$. Conform rezultatului auxiliar demonstrat mai sus avem $h \circ \delta = j$. Deoarece aplicația j este injectivă, rezultă că δ este injectivă și teorema este complet demonstrată. ∎

Observație. Să numim o X-dinamică (D, δ) *liberă relativ la un element* $d \in D$, dacă pentru orice altă X-dinamică (A, δ_1) și oricare ar fi elementul $\alpha \in A$, există și este unic un morfism de dinamici $h : (D, \delta) \to (A, \delta_1)$ astfel încît $h(d) = \alpha$.

Atunci teorema 1.8 se enunță pe scurt astfel : *O X-dinamică (D, δ) este liberă relativ la un element $d \in D$, dacă și numai dacă $(D, \delta)_d$ este o X-dinamică Peano.* Dacă $X = \mathbb{1}$, regăsim teorema 1.1 : mulțimea $\mathbb{N}$ este o $\mathbb{1}$-dinamică liberă relativ la elementul $0 \in \mathbb{N}$.

Rezultatul următor justifică introducerea X-dinamicilor Peano pentru caracterizarea monoizilor liber generați de X.

LEMA 5. *Fie $(D, \cdot, e)$ un monoid și $i : X \to D$ o aplicație de mulțimi. Definim $\delta : D \times X \to D$, $(u, x) \mapsto u \cdot i(x)$. Atunci afirmațiile următoare sînt echivalente :*

(i) *D împreună cu $i : X \to D$ este un monoid liber generat de X;*

(ii) $(D, \delta)_s$ *este o* X*-dinamică Peano.*

Demonstrație. (i) $\Rightarrow$ (ii). Aplicăm teorema 1.8. Fie (A, δ_1) o X-dinamică și $\alpha \in A$. Considerăm monoidul A^A (relativ la compunere și cu elementul neutru 1_A) și fie aplicația

$$g : X \to A^A; \quad \forall x \in X, g(x) : A \to A, a \mapsto \delta_1(a, x)$$

(în general, există o corespondență bijectivă între mulțimile $A^{A\times X}$ și $(A^A)^X$, iar g corespunde lui δ_1). Conform ipotezei, există un morfism de monoizi

$\bar{g} : D \to A^A$ astfel încît $\bar{g} \circ i = g$; așadar, $\bar{g}(uv) = \bar{g}(v) \circ \bar{g}(u)$ și $\bar{g}(e) = 1_A$. Definim

$$h : D \to A, \quad u \mapsto \bar{g}(u)(\alpha).$$

Pentru orice $x \in X$, $u \in D$, avem $[h \circ \delta](u, x) = h(\delta(u, x)) = h(u \cdot i(x)) = \bar{g}(u \cdot i(x))(\alpha) = \bar{g}(ix)(\bar{g}(u)(\alpha)) = g(x)(\bar{g}(u)(\alpha))$ și, pe de altă parte, $[\delta_1 \circ (h \times 1_X)](u, x) = \delta_1(h(u), x) = \delta_1(\bar{g}(u)(\alpha), x) = g(x)(\bar{g}(u)(\alpha))$. Așadar, $h \circ \delta = \delta_1 \circ (h \times 1_X)$ deci h este un morfism de X-dinamici; în plus, $h(e) = \bar{g}(e)(\alpha) = 1_A(\alpha) = \alpha$. Rămîne să dovedim unicitatea lui h; vom demonstra mai întîi, prin inducție monoidală după u (pe care o putem folosi conform lemei 4), că pentru orice $u \in D$ și pentru orice morfism de dinamici $f : (D, \delta) \to (A, \delta_1)$ are loc relația

$$(*) \qquad f(u) = \bar{g}(u)(f(e)).$$

Această relație se verifică pentru $u = i(x)$, $x \in X$, deoarece $\bar{g}(i(x))(f(e)) = g(x)(f(e)) = \delta_1(f(e), x) = f(\delta(e, x)) = f(e \cdot i(x)) = f(i(x))$. Apoi, pentru $u = e$, $\bar{g}(e)(f(e)) = 1_A(f(e)) = f(e)$ și relația are de asemenea loc. În fine, să presupunem că relația se verifică pentru u, $v \in D$ dați și o demonstrăm și pentru uv. Oricare ar fi morfismul de X-dinamici $f : (D, \delta) \to (A, \delta_1)$, aplicația $f_u : (D, \delta) \to (A, \delta_1)$, $v \mapsto f(uv)$ este de asemenea un morfism de X-dinamici și, conform ipotezei,

$$f(uv) = f_u(v) = \bar{g}(v)(f_u(e)) = \bar{g}(v)(f(u)) = \bar{g}(v)(\bar{g}(u)(f(e)) = \bar{g}(uv)(f(e)).$$

Relația $(*)$ este demonstrată. Atunci pentru orice morfism de X-dinamici $f : (D, \delta) \to (A, \delta_1)$ astfel încît $f(e) = \alpha$ avem $\forall u \in D$,

$$f(u) = \bar{g}(u)(f(e)) = \bar{g}(u)(\alpha) = h(u), \quad \text{adică } f = h.$$

(ii) $\Rightarrow$ (i). Fie $(M, \cdot, e')$ un monoid oarecare și $p : X \to M$ o aplicație de mulțimi. Ca și D, M poate fi organizat ca X-dinamică prin $\delta' : M \times X \to M$, $(m, x) \mapsto m \cdot p(x)$. Conform ipotezei (și aplicînd teorema 1.8), există și este unic un morfism de X-dinamici $\bar{p} : (D, \delta) \to (M, \delta')$ astfel încît $\bar{p}(e) = e'$. Așadar, $\bar{p}(w \cdot i(x)) = \bar{p}(w) \cdot p(x)$ pentru orice $w \in M$, $x \in X$. Arătăm, prin inducție succesivă după v, că are loc afirmația următoare:

$$(**) \qquad \forall u \in D, \quad \bar{p}(u \cdot v) = p(u) \cdot \bar{p}(v).$$

Mai întîi, pentru orice $v = e$, avem $p(ue) = \bar{p}(u) \quad p(u) \cdot e' = \bar{p}(u) \cdot \bar{p}(e)$. Fie apoi $v \in D$, astfel încît $\bar{p}(uv) = \bar{p}(u) \cdot p(v)$. Atunci pentru orice $x \in X$, $p(u \cdot \delta(v, x)) = \bar{p}(u \cdot v \cdot i(x)) \quad p(uv) \cdot p(x) = \bar{p}(u) \cdot \bar{p}(v) \cdot p(x) = \bar{p}(u) \cdot \bar{p}(v \cdot i(x)) = \bar{p}(u) \cdot p(\delta(v, x))$ și afirmația (**) rezultă.

Relația (**) arată că $\bar{p}$ este un morfism de monoizi; în plus, $\forall x \in X, \bar{p}(i(x)) = \bar{p}(e \cdot i(x)) = \bar{p}(e) \cdot p(x) = e' \cdot p(x) = p(x)$, deci $\bar{p} \circ i = p$.

Unicitatea morfismului $\bar{p}$ se deduce din faptul că pentru orice morfism de monoizi $q : D \to M$ astfel încît $q \circ i = p$, avem $\forall x \in X$, $\forall u \in D$, $q(\delta(u, x)) = q(u \cdot i(x)) = q(u) \cdot q(i(x)) = q(u) \cdot p(x) = \delta'(q(u), x) = [\delta' \circ (q \times 1_X)](u, x)$, deci $q \circ \delta = \delta' \circ (q \times 1_X)$ și q este un morfism de X-dinamici, deci $q = \bar{p}$ (pentru că, în plus, $q(e) = e'$, deoarece q este morfism de monoizi). ∎

TEOREMA 1.9. *Fie D o mulțime. Aplicația care asociază oricărei structuri de monoid pe D (cu elementul neutru e) și oricărei funcții $i : X \to D$, X-dinamica $\delta : D \times X \to D$, $(u, x) \mapsto u \cdot i(x)$ și elementul $e \in D$, realizează o corespondență bijectivă între monoizii liber generați de X și X-dinamicile Peano cu același suport, anume D.*

Demonstrație. Conform lemei 5, dacă D împreună cu $i : X \to D$ este un monoid liber generat de X, atunci $(D, \delta)_e$ este o X-dinamică Peano; așadar, se asociază oricărei structuri de monoid liber generat de X pe D o structură de X-dinamică Peano pe D.

Fie acum $(D, \delta^*)_d$ cu $d \in D$ o X-dinamică Peano; vom introduce o structură de monoid pe D generalizînd modul de introducere a structurii aditive pe o dinamică Peano (p. 25). Pentru orice $u \in D$ notăm cu $\varphi_u : (D, \delta^*) \to (D, \delta^*)$ unicul morfism de X-dinamici astfel încît $\varphi_u(d) = u$ și definim

$$u \cdot v = \varphi_u(v), \quad \text{pentru orice } u, v \in D.$$

Avem $u \cdot d = \varphi_u(d) = u$ și, cum φ_u este morfism, $u \cdot \delta^*(v, x) = \delta^*(u \cdot v, x)$ pentru orice $u, v \in D$, $x \in X$; în particular, $\delta^*(u, x) = u \cdot \delta^*(d, x)$.

Prin inducție succesivă după v se arată că $\forall u \in D$, $d \cdot u = u$ și prin inducție succesivă după $w \in D$, că $\forall u, v \in D$, $(u \cdot v) \cdot w = u \cdot (v \cdot w)$.

Avem așadar o structură de monoid pe D cu elementul neutru d; în plus, definim aplicația

$$i : X \to D, \quad x \mapsto \delta^*(d, x).$$

Atunci $\forall u \in D, x \in X$, $\delta^*(u, x) = u \cdot i(x)$. Prin urmare, orice X-dinamică Peano pe D se obține dintr-o structură de monoid liber generat de X pe D prin aplicația din enunț.

Să presupunem acum că avem două structuri de monoid liber generat de X pe D, anume $(D, \cdot, d)$ cu $i : X \to D$ și $(D, *, d')$ cu $i' : X \to D$, cărora le este asociată aceeași X-dinamică $\delta : D \times X \to D$ și același element $e \in D$. În primul rînd, $d = d' = e$; apoi, $\forall x \in X$, $i(x) = e \cdot i(x) = \delta(e, x) = e \cdot i'(x) = i'(x)$, deci $i = i'$. Conform lemei 5, $(D, \delta)_e$ este o X-dinamică Peano, deci putem folosi inducția succesivă pe D. Pentru orice $u \in D$ arătăm că $\forall v \in D$, $u \cdot v = u * v$. [Într-adevăr, pentru $v = e$ avem $u \cdot v = u \cdot e = u = u * e = u * v$, iar dacă $v \in D$ satisface $u \cdot v = u * v$, atunci $\forall x \in X$ avem $u \cdot \delta(v, x) = \delta(u \cdot v, x) = \delta(u * v, x) = u * \delta(v, x)$.] Așadar, cele două structuri de monoid liber generat de X pe D coincid. ■

Observație. Corespondența stabilită în teorema 1.9 are proprietatea că dacă $(D', \cdot, e')$ este un monoid, $i' : X \to D'$ o funcție și $f : D \to D'$ un morfism de monoizi cu $f \circ i = i'$, atunci $f : (D, \delta) \to (D', \delta')$ este un morfism de X-dinamici și $f(e) = e'$.

În limbaj de categorii și functori (care va fi precizat în capitolul 3), această corespondență definește un functor; teorema 1.9 afirmă faptul că acest functor stabilește o bijecție între obiecte inițiale.

Teorema de caracterizare intrinsecă

Stabilim acum rezultatul principal al acestui paragraf, într-un cadru teoretic — ansamblist, care nu folosește existența mulțimii $\mathbb{N}$, adică axioma infinitului (vezi § 2.1). Rezultatul a fost obținut în colaborare cu V. Breazu.

TEOREMA 1.10. *Fie X un alfabet, $(D, \cdot, e)$ un monoid și o aplicație de mulțimi $i : X \to D$. Sînt echivalente următoarele afirmații:*

a) *D împreună cu i este un monoid liber generat de X;*

b) *Au loc următoarele proprietăți:*

(b_1) *aplicația i este injectivă;*

(b_2) $e \notin i(X)$;

(b_3) $\forall u, v \in D$, $u \cdot v = e \Rightarrow u = e$ și $v = e$;

(b_4) $\forall\, u,\ v \in D,\ u \cdot v \in i(X) \Rightarrow \{u \in i(X),\ v = e\}$ *sau* $\{u = e,\ v \in i(X)\}$;

(b_5) $\forall\, u, v, u', v' \in D, u \cdot v = u' \cdot v' \Rightarrow \exists\, w \in D$ *astfel încît* $u = u' \cdot w, v' = w \cdot v$ *sau* $u' = u \cdot w, v = w \cdot v'$;

(b_6) $\overline{i(X)} = D$ (*sau, echivalent, orice submonoid al lui* D *care conține* $i(X)$ *coincide cu* D).

Înainte de a da demonstrația, considerăm binevenite cîteva comentarii. Monoizii care satisfac condiția (b_5) se numesc *echidivizibili* și sînt folosiți în teoria automatelor ([13]). Condițiile (b_2) și (b_3) se referă la modul limitat în care elementele lui X pot fi calculate, iar condițiile (b_4) și (b_5) descriu relația între diferitele moduri de calcul al unui element; în fine, (b_6) constituie esența inducției monoidale pe D.

Reamintim axiomele clasice ale lui Peano (în $\mathbb{N}$):

(p_1) 0 nu poate fi un succesor;

(p_2) dacă m este succesor al lui n și p, atunci $n = p$;

(p_3) inducția pe numere naturale;

Din cauza unei apropieri structurale între (b_1)—(b_6) și (p_1)—(p_3), proprietățile (b_1)—(b_6) pot fi numite un **sistem de axiome de tip Peano** pentru D și constituie extinderea axiomelor Peano de la $\mathbb{1}$-dinamici la X-dinamici. N. Răbâncă a avut ideea extinderii teoremei 1.10 la algebre liber generate peste o signatură oarecare.

Demonstrație. Considerăm aplicația

$$\delta : D \times X \to D, \quad (u, x) \mapsto u \cdot i(x).$$

Conform lemei 5, afirmația a) este echivalentă cu faptul că $(D, \delta)_e$ este o X-dinamică Peano. În notațiile monoidului, afirmația a) este deci echivalentă cu conjuncția, pe care o notăm a') a următoarelor trei proprietăți din definiția 1.14:

(a_1) $\forall\, u \in D,\ \forall\, x \in X,$ *avem* $u \cdot i(x) \neq e$;

(a_2) $\forall\, u, v \in D,\ \forall\, x, y \in X, u \cdot i(x) = v \cdot i(y) \Rightarrow u = v$ *și* $x = y$;

(a_3) *dacă* $S \subset D$ *este o parte astfel încît* $e \in S$ *și* $\forall\, (w, x) \in S \times X$, *să avem* $w \cdot i(x) \in S$, *atunci* $S = D$.

Din (a_3) decurge principiul inducției succesive pe D, pe care îl vom folosi tot în notațiile monoidului.

a') $\Rightarrow$ (b). În primul rînd demonstrăm, prin inducție succesivă după u, afirmația

(*) $\forall\, u \in D,\ u \neq e \Rightarrow \exists\, w \in D,\ y \in X$ astfel încît $u = w \cdot i(y)$.

Pentru $u = e$ afirmația este adevărată (falsul implică orice!). Apoi, dacă afirmația este adevărată pentru $u \in D$, atunci $\forall\, x \in X$ ea este adevărată pentru $u \cdot i(x)$, deoarece $u \cdot i(x) = w \cdot i(y)$, luînd $w = u$, $y = x$ (ipoteza de inducție nu intervine de fapt).

a') $\Rightarrow$ (b_1) rezultă din (a_2) luînd $u = v = e$.

a') $\Rightarrow$ (b_2) rezultă astfel: dacă, prin absurd, $e = i(x)$, cu $x \in X$, atunci $e = e \cdot i(x)$ și se contrazice ipoteza (a_1).

a') $\Rightarrow$ (b_3). Fie $u, v \in D$, $u \cdot v = e$. Dacă $v \neq e$, atunci conform afirmației (*), $v = w \cdot i(y)$ cu $w \in D$, $y \in X$, deci $e = u \cdot v = u \cdot w \cdot i(y)$, ceea ce contravine lui (a_1). Așadar, rezultă $v = e$, de unde $u = e$.

a') $\Rightarrow$ (b_4). Fie $u, v \in D$, $u \cdot v \in i(X)$. Apar două cazuri: sau $v = e$ și $u \in i(X)$, sau $v \neq e$ și atunci conform (*), $v = w \cdot i(y)$, deci $u \cdot v = u \cdot w \cdot i(y) \in i(X)$. Ca atare, există $x \in X$ astfel încît $u \cdot w \cdot i(y) = i(x)$. Conform ($a_2$), rezultă $u \cdot w = e$ și $x = y$ și, conform (b_3), $u = w = e$ și $v = e \cdot i(y) = i(y) \in i(X)$.

a') $\Rightarrow$ (b_5). Fixăm $u, u' \in D$ arbitrare și demonstrăm, prin inducție succesivă după v, afirmația următoare:

(**) $\forall\, v \in D$, avem $\{v' \in D, u \cdot v = u' \cdot v' \Rightarrow \exists\, w \in D$ astfel încît

$$u = u' \cdot w, \quad v' = w \cdot v \quad \text{sau} \quad u' = u \cdot w, \quad v = w \cdot v'\}.$$

Pentru $v = e$ avem $u = u' \cdot v'$ și luăm $w = v'$. Demonstrăm apoi afirmația pentru $v \cdot i(x)$, presupunînd-o adevărată pentru v; într-adevăr, dacă $u \cdot (v \cdot i(x)) = u' \cdot v'$, atunci apar două cazuri:

1) $v' = e$ și luăm $w = v \cdot i(x)$. Deci $u' = u \cdot w$ și $v \cdot i(x) = w = w \cdot v'$.

2) $v' \neq e$ și, conform (*), există $w' \in D$, $y \in X$, astfel încît $v' = w' \cdot i(y)$, deci $u \cdot v \cdot i(x) = u' \cdot w' \cdot i(y)$. Conform ($a_2$) rezultă $u \cdot v = u' \cdot w'$ și $x = y$; aplicînd apoi ipoteza de inducție, există $w \in D$ astfel încît $u = u' \cdot w$, $w' = w \cdot v$ sau $u' = u \cdot w$, $v = w \cdot w'$. Dacă însă $w' = w \cdot v$, atunci $v' = w' \cdot i(y) = w \cdot v \cdot i(y) = w \cdot v \cdot i(x)$ iar $u = u' \cdot w$ și afirmația (**) este demonstrată.

a') $\Rightarrow$ (b_6). $\overline{i(X)}$ fiind un submonoid avem $e \in \overline{i(X)}$ și $\forall\, u \in \overline{i(X)}$, $\forall\, x \in X$, $u \cdot i(x) \in \overline{i(X)}$. Conform ($a_3$) va rezulta $\overline{i(X)} = D$.

Demonstrăm acum implicația inversă b) $\Rightarrow$ a).

b) $\Rightarrow$ (a_1). Dacă $u \cdot i(x) = e$, atunci conform (b_3) rezultă $u = e$ și $i(x) = e$, ceea ce contravine lui (b_2).

b) $\Rightarrow$ (a_2). Presupunem că $u, v \in D$ și $x, y \in X$, iar $u \cdot i(x) = v \cdot i(y)$. Atunci, conform ($b_5$), există $w \in D$ astfel ca $u = v \cdot w$,

$i(y) = w \cdot i(x)$ sau $v = u \cdot w$, $i(x) = w \cdot i(y)$. Dacă $u = v \cdot w$ și $i(y) = w \cdot i(x)$, atunci $w \cdot i(x) \in i(X)$ și, conform (b_4), (b_2) și (b_1), rezultă $w = e$, deci $u = v$ și $x = y$.

b) $\Rightarrow (a_3)$. Fie $S \subset D$ astfel încît $e \in S$ și $\forall x \in X$, $S \cdot i(x) \subset S$. Arătăm, mai întîi, că $\forall u \in D$, $z \in S$, avem $zu \in S$. [Datorită ipotezei (b_6) putem folosi pentru aceasta inducția monoidală după u. Pentru $u = e$ afirmația este evidentă. Apoi, pentru orice $x \in S$, $z \in S$, avem $zi(x) \in S$, conform ipotezei asupra lui S. Iar dacă $u, v \in D$ și $z_1, z_2 \in S$, avem $z_1 u \in S$ și $z_2 v \in S$, atunci $\forall z \in S$ avem $z \cdot (u \cdot v) = (z \cdot u) \cdot v \in S$.]

Datorită proprietății tocmai demonstrate, rezultă că $\forall u, v \in S$ avem $u \cdot v \in S$ și, conform ipotezei asupra lui S, $e \in S$ și $\forall x \in X$, $i(x) = e \cdot i(x) \in S$. Așadar, S este un submonoid al lui D care conține $i(X)$. În concluzie, conform ipotezei (b_6), rezultă $S = D$. Teorema este astfel complet demonstrată.

§ 1.5. SERII FORMALE ȘI APLICAȚII ÎN STUDIUL UNOR SISTEME DISCRETE

În acest paragraf vom da cîteva proprietăți ale seriilor formale, îndeosebi în variabile necomutative, cu aplicații semnificative în studiul unor clase de sisteme neliniare. Sînt necesare cîteva pregătiri.

Serii formale

Fie $(A, +, \cdot, 0, 1)$ un semiinel. Un monoid $(V, +, 0)$ se numește un *A-semimodul*, dacă este definită o operație externă $A \times V \to V$, $(a, v) \mapsto av$, cu proprietățile următoare:

1) $\forall a \in A$, $\forall v, w \in V$, $a(v + w) = av + aw$;

2) $\forall a, b \in A$, $\forall v \in V$, $(a + b)v = av + bv$;

3) $\forall a, b \in A$, $\forall v \in V$, $a(bv) = (ab)v$;

4) $0v = 0$ și $1v = v$, pentru orice $v \in V$.

Se definesc în mod natural sub-semimodulele și morfismele de semimodule.

Exemple. 1) Dacă A este un inel, atunci el este un semiinel și orice A-modul este și un A-semimodul. În particular, orice spațiu vectorial peste un corp K este un K-semimodul.

2) Fie $S \subset V$ o submulțime a unui A-semimodul V. Atunci mulțimea tuturor combinațiilor finite de forma $a_1 v_1 + \ldots + a_k v_k$ cu $a_1, \ldots, a_k \in A$ și $v_1, \ldots, v_k \in S$ este un sub-semimodul al lui V, notat $\tilde{S}$; el este cel mai mic sub-semimodul al lui V care conține S și este numit sub-semimodulul *general de S*.

DEFINIȚIA 1.15. Fie A un semiinel și $(M, \cdot, e)$ un monoid. Se numește *serie formală de puteri (cu coeficienți în A, în variabile din M)* orice aplicație de mulțimi

$$s : M \to A.$$

Fie $s_m = s(m)$ pentru orice $m \in M$. Așadar, seria s este tocmai familia $\{s_m\}_{m \in M}$ de elemente din A, indexată după M. Se mai scrie :

$$s = \sum_{m \in M} s_m \cdot m \quad \text{în loc de} \quad s = \{s_m\}_{m \in M}.$$

Mulțimea tuturor seriilor formale de puteri (pe scurt, s.f.) se notează cu $A \langle\langle M \rangle\rangle$. Două s.f.

$$s = \sum_{m \in M} s_m \cdot m, \qquad t = \sum_{m \in M} t_m \cdot m$$

sînt *egale*, dacă și numai dacă $\forall\, m \in M$, $s_m = t_m$. Seria *nulă* este seria $s = 0$ în care toți coeficienții sînt nuli : $s_m = 0$ pentru orice $m \in M$. Pentru orice $a \in A$ se definește *seria constantă*

$$ae = \sum_{m \in M} s_m \cdot m, \quad \text{unde} \quad s_m = \begin{cases} 0 & \text{dacă} \quad m \neq e, \\ a & \text{dacă} \quad m = e. \end{cases}$$

Pentru orice $a \in A$, $w \in M$, se definește seria formală

$$aw = \sum_{m \in M} s_m \cdot m, \text{ unde } \quad s_m = \begin{cases} 0 & \text{dacă} \quad m \neq w, \\ a & \text{dacă} \quad m = w. \end{cases}$$

Se pot defini două aplicații injective naturale.

$$u : A \to A \langle\langle M \rangle\rangle, \quad a \mapsto ae\,; \quad v : M \mapsto A \langle\langle M \rangle\rangle, \quad m \mapsto 1m.$$

Pentru orice s.f. $s = \sum_{m \in M} s_m \cdot m$ mulțimea $\operatorname{supp} s = \{m \in M \mid s_m \neq 0\}$ se numește *suportul* lui s. Dacă mulțimea $\operatorname{supp} s$ are doar un număr finit de elemente, atunci seria s se numește *polinom formal*.

Dacă $s, t \in A \langle\langle M \rangle\rangle$, atunci se definește *suma* $s + t$ ca fiind seria formală $\sum_{m \in M} (s_m + t_m) \cdot m$, iar dacă $\alpha \in A$, se pune $\alpha s = \sum_{m \in M} (\alpha s_m) \cdot m$. Se verifică imediat că mulțimea $A \langle\langle M \rangle\rangle$ este un A-semimodul.

Dacă $(M, \cdot, e)$ este un monoid cu proprietatea că orice element $m \in M$ are doar un număr finit de descompuneri de forma $m = m_1 \cdot m_2$ cu $m_1, m_2 \in M$, atunci pentru orice două s.f. $s, t \in A\langle\langle M\rangle\rangle$ se definește *produsul Cauchy* st ca fiind seria formală

$$st = \sum_{m \in M} c_m \cdot m, \quad \text{unde} \quad c_m = \sum s_{m_1} \cdot t_{m_2},$$

suma făcîndu-se după toate descompunerile posibile $m_1 \cdot m_2 = m$. În acest caz, se verifică ușor că $A\langle\langle M\rangle\rangle$ *este un semiinel relativ la suma de serii formale și produsul Cauchy.*

Ca mulțimi avem $A\langle\langle M\rangle\rangle = A^M$ dar pe $A\langle\langle M\rangle\rangle$ se presupun în plus definite operații algebrice (adunare, înmulțire etc.).

Exemple. 1) Fie $A = \mathbb{R}$ și $M = (\mathbb{N}, +, 0)$. În acest caz, $A\langle\langle M\rangle\rangle$ este un inel notat cu $\mathbb{R}[[X]]$. În loc de $\sum_{n \in \mathbb{N}} s_n \cdot n$ se scrie $\sum_{n \in \mathbb{N}} s_n X^n$ și se obțin astfel seriile de puteri uzuale, cu coeficienți reali. Polinoamele uzuale din $\mathbb{R}[X]$ sînt tocmai seriile formale cu suport finit.

2) Fie X un alfabet finit (nevid). Atunci monoidul $M = (X^*, j, \wedge)$ are proprietatea că orice cuvînt $w \in X^*$ admite doar un număr finit de reprezentări ca juxtapunere de subcuvinte $w = w_1 w_2 = j(w_1, w_2)$ cu $w_1, w_2 \in X^*$. Ca atare, pentru orice semiinel A se poate considera semiinelul $A\langle\langle X^*\rangle\rangle$.

Dacă $X = \mathbb{1}$, atunci monoidul X^* este izomorf cu $(\mathbb{N}, +, 0)$ și regăsim exemplul anterior (pentru $A = \mathbb{R}$). Dacă $|X| \geqslant 2$, atunci elementele lui $A\langle\langle X^*\rangle\rangle$ se mai numesc serii formale *în variabile necomutative.*

Pentru orice $s \in A\langle\langle X^*\rangle\rangle$ suportul ei este un limbaj în alfabetul X, deoarece supp $s \subset X^*$; invers, dacă $L \subset X^*$ este un limbaj oarecare, atunci seria formală

$$s = \sum_{c \in X^*} s_c \cdot c, \quad \text{unde} \quad s_c = \begin{cases} 1 & \text{dacă } c \in L, \\ 0 & \text{dacă } c \notin L \end{cases}$$

se numește seria caracteristică a limbajului L; evident, supp $s = L$.

Seriile formale au multe aplicații în matematica discretă, legate mai ales de studiul gramaticilor, limbajelor formale și automatelor ([13], [46], [34]). În cele ce urmează vom da cîteva aplicații ale seriilor formale, îndeosebi în analiza unor sisteme neliniare.

Fie A un semiinel și X un alfabet finit nevid. O serie formală $s \in A\langle\langle X^*\rangle\rangle$, $s = \sum_{c \in X^*} s_c \cdot c$ se numește *A-recognoscibilă*, dacă există $n \in \mathbb{N}$, $n \geqslant 1$ și o aplicație $\mu : X^* \to M_n(A)$ (matricile $n \times n$ cu coeficienți în A) astfel încît:

$$1)\ \mu(\wedge) = U_n = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix};$$

$$2)\ \forall\, c_1, c_2 \in X^*, \quad \mu(c_1 c_2) = \mu(c_1) \cdot \mu(c_2);$$

3) există o matrice-linie $\lambda \in M_{1,n}(A)$ și o matrice coloană $\gamma \in M_{n,1}(A)$ cu proprietatea că $\forall\, c \in X^*$, $s_c = \lambda \cdot \mu(c) \cdot \gamma$ (în A).

Se mai scrie $s = (n, \mu, \lambda, \gamma)$. Mulțimea seriilor A-recognoscibile se notează cu $\mathrm{Rec}_A(X)$.

Prezentăm cîteva proprietăți.

a) Orice combinație liniară finită de serii A-recognoscibile este o serie de același tip. [Într-adevăr, dacă $s = (n, \mu, \lambda, \gamma)$ și $a \in A$, atunci $as = (n, \mu, a\lambda, \gamma)$ și $sa = (n, \mu, \lambda, \gamma a)$, iar dacă $s' = (n', \mu', \lambda', \gamma')$, atunci $s + s' = (n + n', \mu_1, \lambda_1, \gamma_1)$, unde $\mu_1 = \mathrm{diag}(\mu, \mu')$, $\lambda_1 = (\lambda \mid \lambda')$ și $\gamma_1 = \begin{pmatrix} \gamma \\ \gamma' \end{pmatrix}$.]

b) O serie $s \in A\langle\langle X^* \rangle\rangle$ este recognoscibilă, dacă și numai dacă există $n \geqslant 1$, $\mu : X^* \to M_n(A)$, astfel ca $\mu(\wedge) = U_n$ și $\forall\, c_1, c_2 \in X^*$, $\mu(c_1 c_2) = \mu(c_1) \cdot \mu(c_2)$ și o matrice pătratică $p \in M_n(A)$ astfel încît $\forall\, c \in X^*$, $s_c = \mathrm{Tr}\,(p \cdot \mu(c)) = \sum_{i,j=1}^{n} p_{ij} \mu(c)_{ij}$ ($\mathrm{Tr}\, M$ = urma matricii M).

[Într-adevăr, dacă $s = (n, \mu, \lambda, \gamma)$ se definește $\mu' : X^* \to M_{n+2}(A)$ punînd $\mu'(\wedge) = U_{n+2}$ și

$$\mu'(x) = \left(\begin{array}{c|c|c} 0 & \lambda\mu(x) & \lambda\mu(x)\gamma \\ \hline 0 & \mu(x) & \mu(x)\gamma \\ \hline 0 & 0 & 0 \end{array}\right).$$

Prin inducție după lungime, rezultă că

$$\mu'(c)\,\mu'(x) = \left(\begin{array}{c|c|c} 0 & \lambda\mu(c) & \lambda\mu(c)\gamma \\ \hline 0 & \mu(c) & \mu(c)\gamma \\ \hline 0 & 0 & 0 \end{array}\right) \cdot \left(\begin{array}{c|c|c} 0 & \lambda\mu(x) & \lambda\mu(x)\gamma \\ \hline 0 & \mu(x) & \mu(x)\gamma \\ \hline 0 & 0 & 0 \end{array}\right) =$$

$$= \left(\begin{array}{c|c|c} 0 & \lambda\mu(cx) & \lambda\mu(cx)\gamma \\ \hline 0 & \mu(cx) & \mu(cx)\gamma \\ \hline 0 & 0 & 0 \end{array}\right).$$

Să considerăm acum matricea $p \in M_{n+2}(A)$, $p = (p_{ij})_{1 \leqslant i,j \leqslant n+2}$ punînd $p_{n+2,1} = 1$ și $p_{ij} = 0$ în caz contrar. Atunci $\mathrm{Tr}\,(p\mu'(c)) = \mathrm{Tr}\,(\mu'(c)\,p) = \mu'(c)_{1,n+2} = \lambda\mu(c)\gamma = s_c$, pentru orice $c \in X^*$; reciproc, în condițiile respective cu n, μ fixați pentru orice i, k fixați

considerăm seria recognoscibilă $s_{ik} = (n, \mu, \lambda^{(i)}, \gamma^{(k)})$, unde $\lambda_j^{(i)} = \delta_{ij}$ și $\gamma_l^{(k)} = \delta_{lk}$. Va rezulta $(s_{ik})_c = \mu(c)_{ik}$ și seria s este o combinație liniară de serii din $\mathrm{Rec}_A X$, deci $s \in \mathrm{Rec}_A X$. |

Exemple. 1) Fie $A = \mathbb{Z}$, $X = \{x, y\}$, $n = 2$ și $\mu : X^* \to M_2(\mathbb{Z})$, definit prin $\mu(x) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\mu(y) = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ și extins corespunzător la X^*. Pentru orice $c \in X^*$ avem $\mu(c) = \begin{pmatrix} 1 & |c|_x - |c|_y \\ 0 & 1 \end{pmatrix}$, unde $|c|_x$ este numărul de apariții ale literei x în cuvîntul c. Definim seria formală $s : X^* \to \mathbb{Z}$ prin $s(c) = |c|_x - |c|_y$. Se constată că luînd $\lambda = (1 \quad 0)$ și $\gamma = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ avem $s(c) = \lambda \cdot \mu(c) \cdot \gamma$ pentru orice $c \in X^*$, deci seria s este $\mathbb{Z}$-recognoscibilă; în plus, $\mathrm{supp}\ s = \{c \in X^* \mid |c|_x \neq |c|_y\}$.

2) Fie $X = \{t\}$ și $s = \sum_{n \geqslant 0} s_n t^n \in \mathbb{R}[[t]]$. Presupunem că s este $\mathbb{R}$-recognoscibilă și notăm $M = \mu(t)$. În aceste condiții, conform teoremei Hamilton-Cayley, există $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$ astfel încît $M^r = \alpha_1 M^{r-1} + \alpha_2 M^{r-2} + \ldots + \alpha_r U_r$, unde $\alpha_r = \pm \det M$. Atunci pentru orice $n \geqslant 0$ rezultă $s_{n+r} = \alpha_1 s_{n+r-1} + \alpha_2 s_{n+r-2} + \ldots + \alpha_r s_n$, deci șirul $\{s_n\}_{n \geqslant 0}$ verifică o relație de recurență liniară în r pași. Același lucru are loc și în cazul coeficienților complecși.

Dacă X este un alfabet finit nevid și A este un semiinel, se definește *familia* $\mathrm{Rat}_A(x)$ *a seriilor* A*-raționale peste* X ca fiind cea mai mică familie $\mathcal{R}$ de serii din $A\langle\langle X^* \rangle\rangle$ astfel încît:

1) $\mathcal{R}$ să conțină toate polinoamele formale;

2) dacă $s, t \in \mathcal{R}$, atunci $s + t$, $s \cdot t$ aparțin lui $\mathcal{R}$;

3) dacă $s \in \mathcal{R}$ și $s_\wedge = 0$, atunci seriile $s^+ = \sum_{n \geqslant 1} s^n$ și $1 + s^+$ aparțin lui $\mathcal{R}$.

Notînd cu 1 seria constantă asociată lui $1 \in A$, rezultă că pentru orice $a \in A$, $s \in \mathcal{R}$ avem $as = (a \cdot 1)\, s$ și $a \cdot 1$ fiind un polinom, rezultă că $as \in \mathcal{R}$; în mod similar, $as \in \mathcal{R}$.

Un rezultat profund (teorema Kleene-Schüthzenberger, [47]) afirmă că dacă X este un alfabet finit, atunci pentru orice semiinel A avem $\mathrm{Rat}_A(X) = \mathrm{Rec}_A(X)$. În capitolul IV vom da o extindere acestei teoreme în contextul monoizilor complet ordonați (teorema 4.9). În cazul $A = \mathbb{R}$, $X = \{t\}$, am văzut că acest rezultat revine la faptul că o serie $\sum_{k \geqslant 0} a_k t^k$ este rațională dacă și numai dacă începînd de la un anumit rang, coeficienții a_k satisfac o relație liniară cu coeficienți constanți.

Aplicații

I. *Funcții generatoare.* Pentru orice șir $s = \{a_n\}_{n \geqslant 0}$ de numere complexe se poate considera seria formală de puteri $\sum_{n \geqslant 0} a_n X^n$ din

$\mathbb{C}[[X]]$. Dacă această serie are o rază de convergență $R > 0$, atunci suma ei $f : B(0, R) \to \mathbb{C}$, $f(z) = \sum_{n=0}^{\infty} a_n z^n$ se numește *funcția generatoare* a șirului s. Uneori se numește funcția generatoare a șirului s însăși seria formală asociată. Ideea folosirii seriilor de puteri în probleme combinatorice aparține lui L. Euler (1707-1783).

Exemple. 1) Șirul constant $a_n = 1$, $n \geqslant 0$ admite funcția generatoare $f(z) = \dfrac{1}{1-z}$ definită în bila $B(0, 1)$; șirul $a_n = n$, $n \geqslant 0$, are funcția generatoare $f(z) = \dfrac{z}{(1-z)^2}$ definită de asemenea în $B(0, 1)$. Dar șirul

$$a_n = \begin{cases} n^n, & n \geqslant 1 \\ 0, & n = 0 \end{cases} \quad \text{nu admite funcție generatoare.}$$

Dacă $f : D \to \mathbb{C}$ este o funcție olomorfă într-un deschis $D \subset \mathbb{C}$ astfel încît $0 \in D$, atunci f este funcția generatoare pentru șirul $a_n = \dfrac{f^{(n)}(0)}{n!}$, $n \geqslant 0$.

2) Dacă $s = \{a_n\}_{n \geqslant 0}$, $t = \{b_n\}_{n \geqslant 0}$ sînt șiruri care admit funcțiile generatoare f și g, atunci șirurile $s + t = \{a_n + b_n\}_{n \geqslant 0}$, $\lambda s = \{\lambda a_n\}_{n \geqslant 0}$ ($\lambda \in \mathbb{C}$) și convoluția $s * t = \{c_n\}_{n \geqslant 0}$, $c_n = \sum_{p=0}^{n} a_p b_{n-p}$ au respectiv funcțiile generatoare $f + g$, λf, $f \cdot g$.

3) Să calculăm în cîte moduri un număr $k \in \mathbb{N}$ poate fi scris ca o sumă de puteri naturale ale lui 2 (adică scrierea lui k în baza 2). Euler a avut ideea de a considera seria formală

$$\varphi(z) = (1 + z)(1 + z^2)(1 + z^4)(1 + z^8) \ldots = 1 + A_1 z + A_2 z^2 + \ldots + A_k z^k + \ldots$$

observînd că A_k este tocmai numărul de moduri cerut. Dar $(1 - z)\varphi(z) = 1$, deci

$$\varphi(z) = \frac{1}{1-z} = 1 + z + z^2 + \ldots + z^k + \ldots$$

Așadar, $A_k = 1$ pentru orice $k \geqslant 1$ și descompunerea cerută este unică.

4) Dacă ξ este o variabilă aleatoare cu valori în $\mathbb{N}$, dacă $p_k = P(\xi = k)$, $k \in \mathbb{N}$ și dacă șirul $\{p_k\}_{k \geqslant 0}$ are funcția generatoare $f : B(0, R) \to \mathbb{C}$ definită într-un disc cu $R > 1$, atunci se verifică ușor că media și dispersia lui ξ sînt date prin

$$M\xi = f'(1) \quad \text{și} \quad D\xi = f''(1) + f'(1) - f'(1)^2.$$

De exemplu, dacă ξ este *repartizată Poisson* cu parametrul $\lambda > 0$, adică $p_k = \dfrac{\lambda^k}{k!} e^{-\lambda}$, $k \geqslant 0$, atunci $f(z) = e^{\lambda(z-1)}$ și $M\xi = \lambda$, $D\xi = \lambda$. În mod similar, dacă $n \geqslant 1$, $p \in [0, 1]$ sînt fixate și dacă

$$p_k = \begin{cases} C_n^k p^k (1-p)^{n-k} & \text{pentru } 0 \leqslant k \leqslant n \\ 0 & \text{pentru } k > n \end{cases}$$

, atunci ξ se spune că este *repartizată*

Bernoulli cu parametrul p; în acest caz, $f(z) = (1 + p(z - 1))^n$ și $M\xi = np$, $D\xi = np(1 - p)$.

5) Fie $m \geqslant 1$ un întreg fixat. Pentru fiecare $k \geqslant 1$ întreg căutăm numărul r_k al seturilor distincte $(x_1, \ldots, x_m) \in \mathbb{N}^m$ astfel ca $x_1 + \ldots + x_m = k$. Considerăm seria formală $\psi(z) = (1 + z + z^2 + \ldots)^m = \dfrac{1}{(1 - z)^m}$ și observăm că în $\psi(z)$ coeficientul lui z^k este tocmai numărul r_k cerut. Așadar, $\psi(z) = 1 + r_1 z + r_2 z^2 + \ldots + r_k z^k + \ldots$ Derivînd de k ori (formal) și făcînd $z = 0$ se va obține $r_k = \dfrac{m(m+1)\ldots(m+k-1)}{k!} = C_{m+k-1}^k$.

Să observăm că r_k este totodată numărul tuturor monoamelor de grad k în m nedeterminate.

6) Mai general, să presupunem $m \geqslant 1$ întreg fixat și să considerăm ecuația $a_1 x_1 + a_2 x_2 + \ldots + a_m x_m = k$ cu $a_1, \ldots, a_m \in \mathbb{N}$ date. Să notăm cu γ_k numărul soluțiilor ei în $\mathbb{N}^m$. Considerînd seria formală

$$\psi(z) = (1 + z^{a_1} + z^{2a_1} + z^{3a_1} + \ldots) \cdot (1 + z^{a_2} + z^{2a_2} + z^{3a_2} + \ldots) \ldots (1 + z^{a_m} + z^{2a_m} + z^{3a_m} + \ldots),$$

se observă că

$$\psi(z) = 1 + \gamma_1 z + \gamma_2 z^2 + \ldots + \gamma_k z^k + \ldots.$$

Deoarece

$$\psi(z) = \frac{1}{(1 - z^{a_1})(1 - z^{a_2}) \ldots (1 - z^{a_m})},$$

coeficienții γ_k, $k \geqslant 0$, pot fi calculați efectiv.

O altă problemă clasică este cea a reprezentării numerelor naturale ca sumă de patru pătrate, adică a rezolvării în $\mathbb{N}^4$ a ecuațiilor $x_1^2 + x_2^2 + x_3^2 + x_4^2 = k$ cu $k \in \mathbb{N}$ dat. S. Ramanudjan (1887-1920) a avut ideea considerării seriei formale

$$\varphi(z) = (1 + 2z + 2z^4 + 2z^9 + 2z^{16} + \ldots)^4 = 1 + \pi_1 z + \pi_2 z^2 + \ldots + \pi_k z^k + \ldots$$

observînd că

$$\varphi(z) = 1 + 8 \sum_{\substack{m=1 \\ m \neq 4p}}^{\infty} \frac{mz^m}{1 - z^m}$$

și că π_k este tocmai numărul soluțiilor (x_1, x_2, x_3, x_4) căutate.

Să presupunem acum că șirul $s = \{a_n\}_{n \geqslant 0}$ este dat printr-o relație de recurență liniară în r pași, deci există $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{C}$, $\alpha_r \neq 0$, astfel încît

$$\forall\, n \geqslant 0, \quad a_{n+r} + \alpha_1 a_{n+r-1} + \ldots + \alpha_r a_n = g(n),$$

cu $g : \mathbb{N} \to \mathbb{R}$ funcție dată. Dacă sînt fixate valorile $a_0, a_1, \ldots, a_{r-1}$ (inițializarea!), atunci se deduc succesiv $a_r, a_{r+1}, a_{r+2}, \ldots$. Vom presupune pentru simplificare că $g = 0$. Polinomul

$$P(z) = z^r + \alpha_1 z^{r-1} + \ldots + \alpha_{r-1} z + \alpha_r$$

se numește *polinomul caracteristic* al șirului s și fie $f(z)$ funcția generatoare a lui s. Notînd $Q(z) = z^r \cdot P\left(\frac{1}{z}\right) = 1 + \alpha_1 z + \ldots + \alpha_r z^r$, $Q(z)$ este funcția generatoare a șirului $t = \{1, \alpha_1, \ldots, \alpha_r, 0, 0, \ldots\}$, deci $C = f \cdot Q$ este funcția generatoare a șirului $s * t = \{c_n\}_{n\geqslant 0}$; evident, $C(z) = c_0 + c_1 z + \ldots + c_{r-1}z^{r-1}$ este un polinom de grad cel mult $r-1$ (deoarece $c_{n+r} = a_{n+r} + \alpha_1 a_{n+r-1} + \ldots + \alpha_r a_n = 0$ pentru $n \geqslant 0$, conform relației de recurență). Reținem că $f(z) = \frac{C(z)}{Q(z)}$, cît de polinoame cu gr $C <$ gr Q. Scriind $P(z) = (z - z_1)^{n_1} \ldots (z - z_p)^{n_p}$, $n_1 + \ldots + n_p = n$, rezultă $Q(z) = (1 - zz_1)^{n_1} \ldots (1 - zz_p)^{n_p}$ și $f(z)$ se descompune în fracții simple și se dezvoltă în serie de puteri în jurul originii. Deoarece $f(z) = \sum_{n=0}^{\infty} a_n z^n$, se va deduce expresia termenului general al șirului considerat, care va fi de forma $a_n = \sum_{i=1}^{p} b_i(n)\, z_i^n$.

Exemple. 1) Fie șirul lui Fibonacci $\{a_n\}_{n\geqslant 0}$ definit prin $a_{n+2} - a_{n+1} - a_n = 0$, $n \geqslant 0$ și $a_0 = a_1 = 1$. Înmulțim această relație cu z^{n+2} și rezultă $a_{n+2}z^{n+2} - za_{n+1}z^{n+1} - z^2 a_n z^n = 0$, $n \geqslant 0$, deci $\sum_{n=0}^{\infty} a_{n+2}z^{n+2} - z\sum_{n=0}^{\infty} a_{n+1}z^{n+1} - z^2\sum_{n=0}^{\infty} a_n z^n = 0$. Notînd cu $f(z)$ funcția generatoare a șirului, rezultă

$$(f(z) - a_0 - a_1 z) - z(f(z) - a_0) - z^2 f(z) = 0,$$

deci

$$f(z) = \frac{1}{1 - z - z^2}.$$

Așadar, $f(z) = \frac{1}{\sqrt{5}}\left(\frac{A_1}{1 - A_1 z} - \frac{A_2}{1 - A_2 z}\right)$, unde $A_1 = \frac{1+\sqrt{5}}{2}$ („numărul de aur") și $A_2 = \frac{1-\sqrt{5}}{2}$. Atunci $f(z) = \sum_{n=0}^{\infty} \frac{1}{\sqrt{5}}(A_1^{n+1} - A_2^{n+1})z^n$ și prin urmare $a_n = \frac{1}{\sqrt{5}}(A_1^{n+1} - A_2^{n+1})$, $n \geqslant 0$.

2) Considerăm șirul $\{a_n\}_{n\geqslant 0}$ dat prin $a_{n+2} - 4a_{n+1} + 4a_n = 0$, $n \geqslant 0$ și $a_0 = 1$, $a_1 = 4$. Polinomul caracteristic este $P(z) = z^2 - 4z + 4 = (z-2)^2$ și prin urmare $p = 1$, $z_1 = 2$ și $a_n = (b_0 + b_1 n)\cdot 2^n$. Deoarece $a_0 = 1$, $a_1 = 4$ rezultă $b_0 = 1$, $b_1 = 1$, deci $a_n = (1+n)\cdot 2^n$, $n \geqslant 0$.

3) Pentru a calcula determinantul „tri-bandă"

$$\Delta_n = \begin{vmatrix} 4 & 2 & & & & \\ 2 & 4 & 2 & & 0 & \\ & 2 & & \ddots & & \\ & & & \ddots & \ddots & \\ & & 0 & & \ddots & 2 \\ & & & & 2 & 4 \end{vmatrix}, \quad n \geqslant 1,$$

este suficient să observăm că $\Delta_n = 4\Delta_{n-1} - 4\Delta_{n-2}$, $n \geqslant 2$ și $\Delta_1 = 4$, $\Delta_2 = 12$. Raționînd ca mai sus, rezultă $\Delta_n = (1 + n) \cdot 2^n$.

4) Considerînd alfabetul $X = \{z\}$ și o serie $\sum_{n \geqslant 0} a_n z^n \in \mathbb{C}[[z]]$, presupusă $\mathbb{C}$-recognoscibilă, am văzut atunci că șirul $\{a_n\}_{n \geqslant 0}$ verifică o relație de recurență liniară și reciproc, iar funcția generatoare a acestui șir este rațională.

II. *Sisteme biliniare și serii generatoare.* Se cunoaște rolul transformărilor Fourier și Laplace în studiul fenomenelor liniare staționare. Însă în cazul neliniar sau nestaționar se cunosc puține metode sistematice, conducînd la algoritmi programabili. Seriile formale (în variabile necomutative), permit elaborarea unui calcul simbolic pentru sisteme neliniare jucînd un rol similar celui al funcțiilor de transfer (cît al transformatelor Laplace ale ieșirii și intrării) din cazul sistemelor liniare. Prezentăm cîteva rezultate în acest sens, aparținînd în principal lui M. Fliess [60].

Considerăm un sistem *biliniar* discret descris în spațiul S al stărilor (presupus spațiu vectorial real) prin ecuațiile

$$x(t + 1) = \left(A_0 + \sum_{j=1}^{n} u_j(t) A_j\right) x(t),$$

$$y(t) = \lambda(x(t)), \quad t \in \mathbb{N};$$

$x(0) \in S$ este dat, $A_0, A_1, \ldots, A_n$ sînt aplicații liniare $S \to S$ și $\lambda : S \to \mathbb{R}$ este de asemenea liniară. În fine, $u_1, \ldots, u_n : \mathbb{N} \to \mathbb{R}$ sînt comenzi, iar y este ieșirea pe care o presupunem un scalar real. Dacă $A_0 = 0$ se spune că sistemul este *omogen*. Două sisteme ca mai sus se numesc *indiscernabile* dacă pentru aceleași intrări se obțin aceleași ieșiri; un sistem biliniar se spune că este *realizabil* dacă este indiscernabil de un sistem biliniar avînd spațiul stărilor finit-dimensional.

Exemple. 1) Fie sistemul $\begin{cases} x(t + 1) = u(t) \cdot x(t) \\ y(t) = x(t), \quad t \in \mathbb{N} \end{cases}$ cu $S = \mathbb{R}$, $x(0) = 1$ și $u : \mathbb{N} \to \mathbb{R}$. Ieșirea la momentul t este

$$y(t) = u(t - 1)\, u(t - 2) \ldots u(0)\, x(0).$$

2) Se arată ușor că sistemul liniar

$$x(l+1) = Ax(l) + \sum_{j=1}^{n} u_j(l)\, b_j,$$

$$y(l) = Cx(l)$$

cu spațiul stărilor S, $A : S \to S$ și $C : S \to \mathbb{R}$ aplicații liniare, $b_j \in S$, $1 \leqslant j \leqslant n$, este indiscernabil de un sistem biliniar ca mai sus. În acest caz, dacă $x(0) = 0$, atunci orice ieșire $y(k)$ depinde liniar de comenzile $u_j(l)$, $1 \leqslant j \leqslant n$, $0 \leqslant l \leqslant k-1$; mai precis,

$$y(k) = CA^k x(0) + \sum_{l=1}^{k} \sum_{j=1}^{n} u_j(l-1)\, CA^{k-l} b_j.$$

PROPRIETĂȚI. 1). *Există o bijecție naturală între seriile formale raționale și sistemele discrete biliniare omogene realizabile.*

Pentru demonstrație, să considerăm mai întîi un sistem biliniar omogen realizabil

$$x(t+1) = \left(\sum_{j=1}^{n} u_j(t) A_j \right) \cdot x(t); \quad y(t) = \gamma(x(t)).$$

Pentru orice comenzi $u_1, \ldots, u_n$ avem

$$y(k+1) = \sum_{i_0, \ldots, i_k = 1}^{n} u_{i_k}(k) \ldots u_{i_0}(0)\, \gamma A_{i_k} \ldots A_i\, x(0), \quad k \in \mathbb{N}.$$

Să considerăm alfabetul $X = \{x_1, \ldots, x_n\}$. Atunci putem forma seria rațională $s \in \mathbb{R}\langle\langle X^* \rangle\rangle$ definită prin reprezentarea $\mu : X^* \to M_N(\mathbb{R})$, unde $N = \dim S$ astfel încît $\mu(x_i) = A_i$, $1 \leqslant i \leqslant n$ și $s = \sum_{c \in X^*} (\lambda \mu(c)\, x(0))c$.

Se obține atunci

$$y(k+1) = \sum_{i_0, \ldots, i_k = 1}^{n} s(x_{i_k} \ldots x_{i_0})\, u_{i_k}(k) \ldots u_{i_0}(0), \quad k \in \mathbb{N}.$$

Coeficientul care corespunde cuvîntului vid este $\lambda\, x(0)$ și pentru orice cuvînt $c = x_{i_k} \ldots x_{i_0}$ de lungime $k+1$, coeficientul lui c este egal cu $y(k+1)$ pentru comenzile $u_1, \ldots, u_n$ astfel încît

$$u_{i_0}(0) = 1 \quad \text{și} \quad u_j(0) = 0 \quad \text{pentru} \quad j \neq i_0; \ldots; u_{i_k}(k) = 1 \quad \text{și}$$

$$u_j(k) = 0 \quad \text{pentru} \quad j \neq i_k.$$

Reciproc, fie $s \in \mathbb{R}\langle\langle X^* \rangle\rangle$, unde $X = \{x_1, \ldots, x_n\}$. Conform teoremei Kleene-Schützenberger enunțată anterior, s este $\mathbb{R}$-recognoscibilă, deci există un întreg $N \geqslant 1$, o aplicație $\mu : X^* \to M_N(\mathbb{R})$ și matrici

$\lambda \in M_{1,N}(\mathbb{R})$, $\gamma \in M_{N,1}(\mathbb{R})$ astfel ca $s = \sum_{c \in X^*} (\lambda \mu(c) \gamma) c$. Seriei s îi putem asocia următorul sistem biliniar omogen (zis *generat de* s) :

$$x(t+1) = \sum_{j=1}^{n} u_j(t) \cdot \mu(x_j) \cdot x(t); \quad y(t) = \lambda x(t),$$

având spațiul stărilor $\mathbb{R}^N$ și $x(0) = \gamma$. (Dacă se aleg alte μ, λ, γ se obține un sistem indiscernabil de acesta.)

M. Fliess a demonstrat, mai general, că există o corespondență bijectivă naturală între seriile formale raționale și sistemele biliniare. Ca o consecință, rezultă că orice sistem biliniar neautonom (în care aplicațiile A_i și λ depind de t) este indiscernabil de un sistem biliniar autonom convenabil.

Cele spuse anterior se extind la cazul sistemelor în timp continuu, biliniare realizabile. Să considerăm mai întîi ecuația diferențială

$$\dot{x}(t) = A(t)\, x(t), \quad t \geqslant 0,$$

unde $x(t) \in \mathbb{R}^N$, $x(0)$ dat și $A(t)$ este o matrice $N \times N$ de funcții continue pe porțiuni pe intervalul $[0, +\infty)$. Soluția este dată prin următoarea formulă Peano-Baker :

$$x(t) = \left(U_N + \int_0^t A(\tau)\, \mathrm{d}\tau + \int_0^t A(\tau_1)\, \mathrm{d}\tau_1 \int_0^{\tau_1} A(\tau)\, \mathrm{d}\tau + \right.$$

$$\left. + \int_0^t A(\tau_2)\, \mathrm{d}\tau_2 \int_0^{\tau_2} A(\tau_1)\, \mathrm{d}\tau_1 \int_0^{\tau_1} A(\tau)\, \mathrm{d}\tau + \ldots \right) \cdot x(0);$$

în cazul cînd $A(t)$ este o matrice constantă se regăsește formula

$$x(t) = \left(U_N + \frac{At}{1!} + \frac{A^2 t^2}{2!} + \ldots \right) \cdot x(0) = \mathrm{e}^{At} \cdot x(0).$$

Să considerăm acum un sistem în timp continuu biliniar realizabil

$$\dot{x}(t) = \left(A_0 + \sum_{j=1}^{n} u_j(t) A_j \right) x(t); \quad y(t) = \lambda x(t), \quad t \geqslant 0,$$

cu spațiul stărilor $\mathbb{R}^N$, aplicațiile $A_0, A_1, \ldots, A_n : \mathbb{R}^N \to \mathbb{R}^N$ și $\lambda : \mathbb{R}^N \to \mathbb{R}$ fiind liniare, iar comenzile $u_1, \ldots, u_n : [0, \infty) \to \mathbb{R}$ fiind continue pe porțiuni.

Să punem $\xi_0(t) = t$ și $\xi_i(t) = \int_0^t u_i(\tau)\,\mathrm{d}\tau$, $1 \leqslant i \leqslant n$, deci $\mathrm{d}\xi_0(t) = \mathrm{d}t$, $\mathrm{d}\xi_i(t) = u_i(t)\mathrm{d}t$ și

$$\int_0^t \left(A_0 + \sum_{j_0=1}^{n} u_{j_0}(\tau) A_{j_0}\right) \mathrm{d}\tau = \sum_{j_0=0}^{n} A_{j_0} \int_0^t \mathrm{d}\xi_{j_0},$$

$$\int_0^t \left(A_0 + \sum_{j_k=1}^{n} u_{j_k}(\tau_k) A_{j_k}\right) \mathrm{d}\tau_k \int_0^{\tau_k} \ldots \int_0^{\tau_1} \left(A_0 + \sum_{j_0=1}^{n} u_{j_0}(\tau) A_{j_0}\right) \mathrm{d}\tau =$$

$$= \sum_{j_k, \ldots, j_0}^{n} A_{j_k} \ldots A_{j_0} \int_0^t \mathrm{d}\xi_{j_k} \ldots \mathrm{d}\xi_{j_0} \quad (k \geqslant 1),$$

unde integrala iterată din membrul drept (atașată cuvîntului nevid $x_{j_k} \ldots x_{j_0} \in X^*$) este definită, prin inducție asupra lungimii, astfel: $\int_0^t \mathrm{d}\xi_j = \xi_j(t)$, $j = 0, 1, \ldots, n$ și dacă integrala $I(\tau) = \int_0^\tau \mathrm{d}\xi_{j_{k-1}} \ldots \mathrm{d}\xi_{j_0}$ este definită pentru orice $\tau \geqslant 0$, atunci

$$\int_0^t \mathrm{d}\xi_j \ldots \mathrm{d}\xi_0 = \int_0^t I(\tau)\,\mathrm{d}\xi_{j_k}(\tau) \text{ (în sens Stieltjes).}$$

De exemplu, cuvîntului $x_0^{\alpha_k} x_{i_k} x_0^{\alpha_{k-1}} \ldots x_{i_1} x_0^{\alpha_0}$ $(1 \leqslant i_1, \ldots, i_k \leqslant n)$ îi corespunde integrala iterată

$$\int_0^t \int_0^{\tau_k} \ldots \int_0^{\tau_2} \frac{(t - \tau_k)^{\alpha_k} u_{i_k}(\tau_k) (\tau_k - \tau_{k-1})^{\alpha_{k-1}} \ldots u_{i_1}(\tau_1) \tau_1^{\alpha_0}}{\alpha_k!\, \alpha_{k-1}! \ldots \alpha_0!} \mathrm{d}\tau_k \ldots \mathrm{d}\tau_1$$

care generalizează integrala binecunoscută asociată cuvîntului $x_0^\alpha x_1$, anume $\int_0^t \frac{(t-\tau)^\alpha}{\alpha!} u_1(\tau)\,\mathrm{d}\tau$ (aceasta fiind primitiva de ordin α a lui u_1, care se anulează în origine împreună cu primele α derivate).

Formula Peano-Baker poate fi atunci scrisă mai succint astfel :

$$y(t) = \lambda \left(1 + \sum_{k \geqslant 0} \sum_{j_k, \ldots, j_0 = 0}^{n} A_{j_k} \ldots A_{j_0} \int_0^t d\xi_{j_k} \ldots d\xi_{j_0}\right) x(0),$$

unde 1 este aplicația identică a lui $\mathbb{R}^N$.

Să considerăm alfabetul $X = \{x_0, x_1, \ldots, x_n\}$, unde litera x_j corespunde lui ξ_j deci x_0 corespunde timpului, considerat ca o intrare particulară, iar $x_1, \ldots, x_n$ corespund comenzilor $u_1, \ldots, u_n$. Sistemului considerat anterior i se poate atunci asocia următoarea serie formală rațională $s \in \mathbb{R}\langle\langle X^* \rangle\rangle$ definită prin

$$s = \sum_{c \in X^*} (\lambda \mu(c)\, x(0))\, c,$$

unde $\mu : X^* \to M_N(\mathbb{R})$, $\mu(x_i) = A_i$, $0 \leqslant i \leqslant n$.
Cu aceste notații, avem

$$y(t) = s(\wedge) + \sum_{k \geqslant 0} \sum_{j_k, \ldots, j_0 = 0}^{n} s(x_{j_k} \ldots x_{j_0}) \int_0^t d\xi_{j_k} \ldots d\xi_{j_0}.$$

Reciproc, oricărei serii raționale $s \in \mathbb{R}\langle\langle X^* \rangle\rangle$, deci recognoscibile, definită prin $\mu : X^* \to M_N(\mathbb{R})$, $\lambda \in M_{1,N}(\mathbb{R})$ și $\gamma \in M_{N,1}(\mathbb{R})$ i se asociază sistemul biliniar :

$$\dot{x}(t) = \left(\mu(x_0) + \sum_{j=1}^{n} u_j(t) \cdot \mu(x_j)\right) \cdot x(t);$$

$y(t) = \lambda x(t)$, cu spațiul stărilor $\mathbb{R}^N$ și $x(0) = \gamma$.
(s se numește *seria generatoare* a acestui sistem).

Am demonstrat astfel următorul fapt :

2) *Există o bijecție naturală între seriile formale raționale și sistemele în timp continuu biliniare realizabile.*

Observație. Fie $g \in \mathbb{R}\langle\langle X^* \rangle\rangle$; presupunem că există numere reale pozitive T, M astfel ca seria numerică

$$y(t) = g(\wedge) + \sum_{k \geqslant 0} \sum_{j_k, \ldots, j_0 = 0}^{n} g(x_{j_k} \ldots x_{j_0}) \int_0^t d\xi_{j_k} \ldots d\xi_{j_0}, \quad 0 \leqslant t \leqslant T,$$

să fie absolut convergentă : $\xi_0(\tau) = \tau$, $\xi_i(\tau) = \int_0^\tau u_i(t)\, dt$, $1 \leqslant i \leqslant n$, cu u_i continue pe porțiuni și $\max_{0 \leqslant t \leqslant T} |u_i(t)| \leqslant M$.

Asocierea $g \mapsto y$ este o funcțională (numită *cauzală*) deoarece $y(t)$ nu depinde decît de valorile lui $u_i(\tau)$ cu $\tau \leqslant t$).

Considerăm două sisteme biliniare avînd aceeași intrare scalară u și ieșirile y_1, y_2. *Suma* (resp. *produsul*) lor este sistemul (de același tip) avînd ieșirea $y(t) = y_1(t) + y_2(t)$ (resp. $y_1(t) \cdot y_2(t)$) la orice moment t. Se verifică ușor că seria generatoare a sumei este suma seriilor s_1, s_2 generatoare; în schimb, seria generatoare a produsului este produsul Hurwitz $s = s_1 * s_2$, definit prin $s = \sum_{p, q \in X^*} s_1(p) s_2(q)\ (p * q)$ [unde pentru orice cuvinte $p, q \in X^*$ polinomul formal $p * q$ este definit prin inducție după formulele $\wedge * q = q * \wedge = q$, pentru orice $q \in X^*$ și $px * qy = (px * q)\, y + (p * qy)x$ pentru orice cuvinte $p, q \in X^*$ și orice litere $x, y \in X$].

Exemple. 1) Să considerăm un sistem descris printr-o ecuație integrală neliniară de forma

$$\begin{cases} x(t) = x(0) + ta(t) + \int_0^t \left[f(\tau, x(\tau)) + \sum_{j=1}^{n} u_j(\tau) \cdot g_j(\tau, x(\tau)) \right] d\tau, \\ y(t) = h(t, x(t)), \end{cases}$$

unde vectorul de stare $x(t)$ aparține unui spațiu vectorial real S, dim $S = N$, cu $x(0)$ dat: aici $a : [0, \infty) \to S$ și $f, g_1, \ldots, g_n$ sînt funcții $[0, \infty) \times S \to S$, $h : [0, \infty) \times S \to \mathbb{R}$, toate presupuse funcții analitice într-o vecinătate a lui $t = 0$, $u_1, \ldots, u_n : [0, \infty) \to \mathbb{R}$ sînt comenzi și, în fine, $y \in \mathbb{R}$ este o ieșire.

Ne punem problema să asociem o serie formală generatoare acestui sistem. Fie $X = \{x_0, x_1, \ldots, x_n\}$ și $Z = \{\xi_1, \ldots, \xi_N, \xi_{N+1}\}$ cu $\xi_1, \ldots, \xi_{N+1}$ serii necunoscute din $\mathbb{R}\langle\langle X^* \rangle\rangle$, unde $\xi_1, \ldots, \xi_N$ corespund celor N componente ale stării x și ξ_{N+1} corespunde ieșirii y. Așa cum am văzut, înmulțirea la stînga cu x_0 corespunde operației de integrare, înmulțirea cu x_i corespunde multiplicării cu u_i, urmată de integrare; iar produsului valorilor numerice îi corespunde produsul Hurwitz „$*$" al nedeterminatelor necomutative. Acestea conduc la scrierea matricială

$$\begin{pmatrix} \xi_1 \\ \cdot \\ \cdot \\ \cdot \\ \xi_N \end{pmatrix} = x(0) + x_0 * A(x_0) + x_0 F(x_0, \xi_1, \ldots, \xi_N) + \sum_{j=1}^{n} x_j G_j(x_j, \xi_1, \ldots, \xi_N)$$

$$\xi_{N+1} = H(x_0, \xi_1, \ldots, \xi_N),$$

unde A este o serie în x_0 și $F, G_1, \ldots, G_n, H$ sînt serii în variabilele $x_0, \xi_1, \ldots, \xi_N$; mai precis, seriile $A, F, G_1, \ldots, G_n$, H sînt determinate *via* dezvoltările în serie întreagă ale funcțiilor analitice a, f, $g_1, \ldots, g_n$, h respectiv. Astfel, dacă

$$f(t, q) = \sum_{k_0, k_1, \ldots, k_N \geqslant 0} f_{k_0 \ldots k_N}\, t^{k_0} \cdot q_1^{k_1} \ldots q_N^{k_N}, \quad \text{atunci}$$

$$F = \sum_{k_0 \ldots, k_N \geqslant 0} f_{k_0 \ldots k_N} (x_0 \underbrace{* \ldots *}_{k_0 \text{ ori}} x_0) * (\xi_1 \underbrace{* \ldots *}_{k_1 \text{ ori}} \xi_1) \ldots (\xi_N \underbrace{* \ldots *}_{k_N \text{ ori}} \xi_N).$$

Sistemul matricial anterior se rezolvă prin iterare și seria generatoare a sistemului integro-diferențial considerat inițial este cea de $(N + 1)$-a coordonată a soluției sistemului matricial.

Fie ecuația diferențială liniară cu coeficienți constanți

$$y^{(n)} + a_1 y^{(n-1)} + \ldots + a_{n-1}\dot{y} + a_n y = u(t),$$

unde u este comanda, y ieșirea, cu condițiile inițiale $\dot{y}(0) = y(0) = \ldots y^{(n-1)}(0) = 0$. După n integrări succesive se ajunge la ecuația integrală

$$y(t) + a_1 \int_0^t y(\tau)\,d\tau + \ldots + a_n \int_0^t d\tau_{n-1} \int_0^{\tau_{n-1}} \ldots \int_0^{\tau_1} y(\tau)\,d\tau =$$

$$= \int_0^t d\tau_{n-1} \int_0^{\tau_{n-1}} \ldots \int_0^{\tau_1} u(\tau)\,d\tau.$$

Seria formală generatoare s verifică în acest caz relația

$$s + a_1 x_0 s + \ldots + a_n x_0^n s = x_0^{n-1} x_1,$$

deci $s = (1 + a_1 x_0 + \ldots + a_n x_0^n)^{-1} x_0^{n-1} x_1$. Se constată legătura directă cu funcția de transfer $\Phi(p) = \dfrac{1}{p^n + a_1 p^{n-1} + \ldots + a_n}$ $\left(p = \dfrac{d}{dt},\ x_0 = \displaystyle\int_0^t\right)$

În general, dacă seria generatoare este de forma $\displaystyle\sum_{i=1}^{n} \sum_{k>0} a_{ik} x_0^k x_i$, atunci funcțională cauzală corespunzătoare este $\displaystyle\sum_{i=1}^{n} \int_0^t h_i(t-\tau)\, u_i(\tau)\,d\tau$. Transformata Laplace a lui h_i este

$$\int_0^\infty e^{-p\tau} \cdot h_i(\tau)\,d\tau = \sum_{k>0} \frac{a_{ik}}{p^{k+1}}$$

și se observă legătura existentă între serii generatoare și funcții de transfer. Așadar, seriile generatoare oferă o extindere neliniară a transformării Laplace.

2) Fie ecuația $\dot{y} - y^2 = u(t)$ cu $y(0) = b$ dat. O rescriem sub formă integrală și devine

$$y(t) - \int_0^t y^2(\tau)\,d\tau = \int_0^t u(\tau)\,d\tau + b.$$

Seria generatoare $s \in \mathbb{R}\langle\langle X^* \rangle\rangle$, unde $X = \{x_0, x_1\}$ verifică în acest caz relația

$$s = b + x_1 + x_0(s * s).$$

Rezolvarea acestei ecuații se face prin aproximații polinomiale succesive: $s_0 = b$, $s_1 = b + x_1 + b^2 x_0$, $s_2 = b + x_1 + b^2 x_0 + 2b x_0 x_1 + 2b^3 x_0^2$ etc.

3) Fie sistemul

$$\begin{cases} \dot{x}(t) = Ax(t) + \sum_{j=0}^{n} u_j(t) b_j, \\ y(t) = Cx(t), \end{cases}$$

unde $x(t), b_1, \ldots, b_n$ aparţin unui spaţiu vectorial real S cu $\dim S < \infty$, iar $x(0) = 0$; aplicaţiile $A : S \to S$, $C : S \to \mathbb{R}$ sînt presupuse $\mathbb{R}$-liniare. Seria generatoare asociată este $s = C \cdot (1 - Ax_0)^{-1} \cdot \sum_{j=1}^{n} b_j x_j$, în timp ce matricea de transfer este $C \cdot p \cdot 1 - A)^{-1} \cdot (b_1, \ldots, b_n)^T$. Calculul simbolic cu serii formale generatoare generalizează la cazul neliniar calculul operaţional al lui Heaviside.

CAPITOLUL 2

FINITUDINE ȘI NUMĂRARE

Introducere

În capitolul precedent am studiat problema generării numerelor naturale și, mai general, a șirurilor finite de litere ale unui alfabet. În acest capitol vom reaminti în mod sistematic modul în care numerele naturale sînt utilizate în „măsurarea bogăției" în elemente a mulțimilor finite, prin corespondențe bijective cu mulțimi de forma $S_n = \{x \in \mathbb{N} \mid x < n\}$. Vom demonstra de asemenea cîteva rezultate importante relativ la mulțimi inite, care folosesc în mod esențial raționamente prin inducție și vom stabili echivalența definițiilor Zermelo, Cantor și Dedekind pentru o mulțime infinită, prilej cu care vom discuta problema existenței și construcției obiectelor matematice, a introducerii infinitului în matematică.

Vom demonstra apoi cîteva rezultate de cardinalitate a unor mulțimi (dicționare, limbaje etc.) care apar în matematica discretă, ilustrînd totodată conceptul de numărare. Ultima parte a acestui capitol este consacrată studiului operațiilor algebrice pe mulțimi finite.

§ 2.1. MULȚIMI FINITE

Definiția lui Dedekind

Mulțimile finite apar în multe deserieri și ele sînt importante și pentru că adeseori admit o realizare fizică. Reamintim că pentru orice $p \in \mathbb{N}$ am notat

$$S_p = \{x \in \mathbb{N} \mid x < p\}.$$

Așadar, $S_0 = \emptyset$, $S_1 = \{0\}$ și pentru orice $p \geqslant 2$, $S_p = \{0, 1, \ldots, p-1\}$; în plus, $\forall\, n \in \mathbb{N}$, $S_{s(n)} = S_n \cup \{n\}$. Se observă de asemenea că

$$S_m \subset S_n \leftrightarrow m \leqslant n \text{ și } S_m \underset{\neq}{\subset} S_n \leftrightarrow m < n.$$

DEFINIȚIA 2.1 (Dedekind). Prin *mulțime finită* se înțelege o mulțime echipotentă cu o mulțime de forma S_n cu $n \in \mathbb{N}$.

Un rezultat important îl constituie teorema următoare.

TEOREMA 2.1. *Nu există nici un număr natural* $n \in \mathbb{N}$ *astfel încît mulțimea* S_n *să fie echipotentă* ($\sim$) *cu o parte strictă a ei.*

Demonstrație. Să considerăm mulțimea

$$C = \{n \in \mathbb{N} \mid \exists\, X \underset{\neq}{\subset} S_n,\ X \sim S_n\}.$$

Avem de arătat că această mulțime este vidă. În caz contrar, teorema 1.2 arată că există $p = \min C$. Avem $p \neq 0$, deoarece mulțimea $S_0 = \emptyset$ nu are părți stricte; de asemenea, $p \neq 1$ pentru că $S_1 = \{0\}$ are ca parte strictă doar $\emptyset$. Așadar, $p \geqslant 2$. Fie $p' = p - 1$ și o parte strictă $X \underset{\neq}{\subset} S_p$ echipotentă cu S_p. Fie $g : S_p \to X$ o aplicație bijectivă. Apar trei cazuri:

1. $p' \notin X$. Atunci $X \subset S_{p'}$ și $X \setminus \{g(p')\} \underset{\neq}{\subset} S_{p'}$. Dar $S_{p'}$ este echipotentă cu $X \setminus \{g(p')\}$, deci $p' \in C$, ceea ce contrazice faptul că $p = \min C$.

2. $p' \in X$ și $g^{-1}(p') = p'$. Atunci $X \setminus \{p'\} \underset{\neq}{\subset} S_{p'}$ și $S_{p'}$ este echipotentă cu $X \setminus \{p'\}$, ajungîndu-se la o contradicție.

3. $p' \in X$ și $g^{-1}(p') \neq p'$. În acest caz, există $u \in S_{p'}$ și $u \notin X$ (altminteri, $S_{p'} \subset X \underset{\neq}{\subset} S_p$, deci $X = S_{p'}$ și ar rezulta $p' \in S_{p'}$, absurd). Să luăm $Y = (X \cup \{u\}) \setminus \{p', g(p')\}$. Se poate considera aplicația bijectivă

$$h : S_{p'} \to Y, \quad h(x) = \begin{cases} g(x) & \text{dacă } x \neq g^{-1}(p'), \\ u & \text{dacă } x = g^{-1}(p'), \end{cases}$$

iar incluziunea $Y \subset S_{p'}$ este strictă, deoarece $g(p') \in S_{p'}$ și $g(p') \notin Y$; așadar, $S_{p'}$ ar fi echipotentă cu o parte strictă a ei, adică $p' \in C$, ceea ce contrazice din nou faptul că $p = \min C$. ∎

Dăm acum mai multe consecințe ale teoremei 2.1, folosind doar definiția lui Dedekind a finitudinii.

Proprietăți ale mulțimilor finite

1) *Dacă* M *este o mulțime finită și dacă* $M_1 \sim M$, *atunci* M_1 *este finită.*

Demonstrația este evidentă.

2) *Dacă* M *este o mulțime finită, atunci* $(\exists\,!)\ n \in \mathbb{N}$ *astfel încît* $M \sim S_n$.

Într-adevăr, să presupunem că $M \sim S_n$, $M \sim S_m$, deci $S_m \sim S_n$. Dacă $m < n$ sau dacă $n < m$, atunci $S_m \subsetneq S_n$ și, respectiv, $S_n \subsetneq S_m$, ceea ce contravine teoremei 2.1. Așadar, $m = n$.

Numărul n, unic astfel încît $M \sim S_n$, se numește *numărul de elemente* ale mulțimii finite M și se mai notează cu $|M|$. Evident, dacă mulțimile M_1 și M_2 sînt finite, atunci $M_1 \sim M_2 \leftrightarrow |M_1| = |M_2|$.

3) *Dacă M este finită și $f : S_n \to M$ este o bijecție, atunci* $M = \{f(0), \ldots, f(n-1)\}$.

Evident.

4) *Dacă M este o mulțime finită și $M' \subset M$, atunci M' este finită și* $|M'| \leqslant |M|$.

Este suficient să observăm că dacă $P \subset S_m$, atunci există $m' \leqslant m$ astfel încît $P \sim S_{m'}$.

5) *Fie M și N mulțimi finite. Atunci mulțimea $M \cup N$ este finită și*

$$|M \cup N| = |M| + |N| - |M \cap N|.$$

Demonstrație. Arătăm mai întîi că $\forall\, m, n \in \mathbb{N}$, $(S_{m+n} \setminus S_m) \sim S_n$. Pentru aceasta să observăm că aplicația

$$\pi_m : \mathbb{N} \to \mathbb{N},\ p \mapsto m + p$$

este injectivă și $\pi_m(S_n) = S_{m+n} \setminus S_m$ [Într-adevăr, $\forall\, p \in S_{m+n} \setminus S_n$ avem $m \leqslant p < m + n$, deci există q astfel încît $p = m + q$. Atunci $m + q < m + n$, deci $q < n$, adică $p = \pi_m(q)$ cu $q \in S_n$.]

Să considerăm mai întîi cazul cînd M și N sînt disjuncte; atunci, există $m, n \in \mathbb{N}$ astfel încît $M \sim S_m$, $N \sim S_n \sim S_{m+n} \setminus S_n$, deci $M \cup N \sim S_{m+n}$ și ca atare $M \cup N$ este finită și, în plus, $|M \cup N| = m + n$.

Rezultă că dacă M este finită și $M' \subset M$, atunci M' și $M \setminus M'$ sînt finite și disjuncte, deci $|M \setminus M'| = |M| - |M'|$.

Trecem acum la cazul general; considerînd mulțimile finite și disjuncte M și $N \setminus (M \cap N)$ avînd reuniunea $M \cup N$, rezultă $|M| + |N \setminus (M \cap N)| = |M \cup N|$, adică $|M| + |N| - |M \cap N| = |M \cup N|$. ∎

Reținem așadar că pentru orice două mulțimi finite M, N avem $|M \cup N| \leqslant |M| + |N|$, $|M \cap N| \leqslant \min(|M|, |N|)$ și $|M + N| = |M| + |N|$. De asemenea, se demonstrează imediat că $|M| \leqslant |N| \leftrightarrow$ există o funcție injectivă $M \to N \leftrightarrow$ există o funcție surjectivă $N \to M$.

6) *Dacă M și N sînt mulțimi finite, atunci produsul cartezian $M \times N$ este mulțime finită și*

$$|M \times N| = |M| \cdot |N|.$$

Demonstrație. Este suficient de arătat că

$$\forall\, m, n \in \mathbb{N},\ S_m \times S_n \sim S_{mn}.$$

Dacă $m = 0$ sau $n = 0$, atunci $S_0 = \emptyset$ și afirmația este evidentă. Presupunem că $m \geqslant 1$, $n \geqslant 1$ și observăm că dacă $r \leqslant m - 1$ și $q \leqslant n - 1$, atunci $mq + r \leqslant m(n-1) + m - 1 < mn$. Putem defini prin urmare aplicația

$$\varphi : S_m \times S_n \to S_{mn},\ (r, q) \mapsto mq + r.$$

Arătăm că φ este bijectivă. Pentru orice $a \in S_{mn}$ avem $a < mn$ și aplicînd teorema 1.3, există $q, r \in \mathbb{N}$ astfel ca $a = mq + r$ și $r < m$. Atunci $q < n$ (căci dacă $q \geqslant n$ ar rezulta $mq + r \geqslant mn - r$, deci $a \geqslant mn + r \geqslant mn$) și, evident, $\varphi(r, q) = a$. Deci φ este surjectivă, iar din unicitatea împărțirii cu rest rezultă că φ este și injectivă. ∎

Exemple. 1) Dacă un punct A este unit cu un punct B prin p arce, iar B este unit cu un punct C prin q arce, atunci de la A la C se poate „ajunge" în $p \cdot q$ moduri.

Proprietățile 5), 6) se extind prin inducție la un număr finit oarecare de mulțimi finite. Așadar, pentru orice mulțime finită M și pentru orice $n \in \mathbb{N}$, $|M^n| = |M|^n$.

2) Se consideră toate numerele între 1 și 10^p ($p \geqslant 1$); ne propunem să determinăm cîte dintre ele conțin o anumită cifră zecimală (de exemplu 7). Pentru aceasta calculăm numărul șirurilor de cîte p cifre zecimale distincte de 7; existînd cîte nouă posibilități pentru fiecare termen, numărul acestor șiruri va fi 9^p și răspunsul căutat este $10^p - 9^p$.

3) Reamintim că elementele mulțimii $\mathbb{B}^n$, $n \geqslant 1$, se mai numesc *șiruri de n biți*. Evident,

— numărul șirurilor de n biți este $|\mathbb{B}^n| = 2^n$;

— numărul șirurilor de cel mult n biți este $2 + 2^2 + \ldots + 2^n = 2^{n+1} - 2$.

4) Fie un alfabet $X = \{a_1, a_2, \ldots, a_n\}$ cu $n \geqslant 2$ simboluri. Ne propunem să determinăm numărul cuvintelor nevide care cuprind fiecare simbol cel mult o dată. Mulțimea A a cuvintelor respective este reuniunea (disjunctă) a n mulțimi $A_1, A_2, \ldots, A_n$ cuprinzînd cuvinte de lungime $1, 2, \ldots, n$, respectiv. În acest caz, $|A_1| = n$, $|A_2| = n(n-1), \ldots, |A_k| = A_n^k$ pentru $1 \leqslant k \leqslant n$ și numărul cerut este $c_n = \sum_{k=1}^{n} A_n^k$. Se observă că $\forall\ n \geqslant 2$, $c_n = n(1 + c_{n-1})$ și $c_1 = 1$.

7) *Dacă M este o mulțime finită, atunci mulțimea $\mathbf{p}(M)$ este finită și $|\mathbf{p}(M)| = 2^{|M|}$.*

Demonstrație. Aplicăm inducția după $m = |M|$. Dacă $m = 0$, atunci $M = \emptyset$ și $\mathbf{p}(M) = \{\emptyset\}$ și relația devine $1 = 2^0$. Presupunem afirmația demonstrată pentru mulțimi avînd m elemente și fie M o mulțime cu $m + 1$ elemente. Fie $a \in M$ și $M' = M \setminus \{a\}$. Atunci $\mathbf{p}(M) = \{A \subset M \mid a \in M\} \cup \{A \subset M \mid a \notin M\} = \{B \cup \{a\} \mid B \subset M'\} \cup \mathbf{p}(M')$ și, conform 5), $|\mathbf{p}(M)| = |\mathbf{p}(M')| + |\mathbf{p}(M')| = 2^m + 2^m = 2^{m+1}$.

O altă demonstrație se obține observînd că dacă $0 \leqslant r \leqslant m$, atunci există C_m^r submulțimi cu r elemente ale unei mulțimi M cu m elemente, iar numărul total de submulțimi ale lui M va fi $\sum_{r=0}^{m} C_m^r = (1+1)^m = 2^m$. ∎

8) *Fie M și N două mulțimi finite și $m = |M|$, $n = |N|$. Atunci numărul*

a) *relațiilor binare de la M la N este 2^{mn};*

b) *funcțiilor totale de la M la N este n^m;*

c) *funcțiilor parțiale de la M la N este $(n+1)^m$;*

d) *predicatelor p-are pe M este $2^{(mp)}$.*

Demonstrație. a) Mulțimea relațiilor binare de la M la N este $\mathbf{p}(M \times N)$; conform proprietăților 6), 7) rezultă $|\mathbf{p}(M \times N)| = 2^{|M \times N|} = 2^{mn}$.

b) Avem $N^M \subset \mathbf{p}(M \times N)$, deci mulțimea funcțiilor totale de la M la N este finită; faptul că $|N^M| = n^m$ se demonstrează prin inducție după m.

c) Oricărei funcții parțiale $f : M \to N$ i se poate asocia bijectiv o funcție totală $f^{\perp}$, adjuncționînd mulțimii N un element $\perp \notin N$ și definind $f^{\perp} : M \to N \cup \{\perp\}$, $f^{\perp}(x) = \begin{cases} f(x) & x \in D_f, \\ \perp & x \notin D_f. \end{cases}$

d) Predicatele p-are pe M sînt tocmai funcții $M^p \to \mathbb{B}$ și se aplică b). ∎

Să notăm de asemenea că dacă $m \leqslant n$, atunci numărul aplicațiilor injective $M \rightarrowtail N$ este $\dfrac{n!}{(n-m)!}$, iar numărul aplicațiilor surjective $N \to M$ este egal cu $\sum_{k=0}^{m-1} (-1)^k \cdot C_m^k \cdot (m-k)^n$ ([56]).

Adăugăm încă două proprietăți legate de mulțimile ordonate.

9) *Fie $(M, \leqslant)$ o mulțime ordonată finită. Pentru orice elemente $a < b$ din M există un lanț (șir finit) în M,*

$$x_0 = a < x_1 < \ldots < x_k = b,$$

cu proprietatea că $\forall\, i, 1 \leqslant i \leqslant k$, să avem $x_{i-1} < x_i$, dar să nu existe $y \in M$ astfel încît $x_{i-1} < y < x_i$.

Fie n numărul acelor $y \in M$ astfel încît $a < y < b$. Vom proceda prin inducție după n. Pentru $n = 0$ afirmația este evidentă. Presupunem $n \geqslant 1$ și fie $a < c < b$. Atunci numărul acelor y pentru care

$a < y < c$ și al acelor z pentru care $c < z < b$ este cel mult $n - 1$ (deoarece am exclus pe c). Conform ipotezei de inducție există lanțuri finite unind a cu c și c cu b; reunindu-le se găsește un lanț cu proprietatea din enunț. ∎

10) *Fie* $(M, \leqslant)$ *o mulțime ordonată finită. Atunci elementele lui* M *pot fi dispuse astfel încît* $M = \{x_1, \ldots, x_n\}$ *și* $x_i < x_j \Rightarrow i < j$ (se mai spune că există o enumerare a elementelor lui M compatibilă cu ordinea).

Pentru demonstrație să presupunem, conform 3), că $M = \{a_0, \ldots, a_{n-1}\}$; notăm $M_k = \{a_0, \ldots, a_{k-1}\}$ pentru $1 \leqslant k \leqslant n$. Vom construi inductiv aplicații bijective $\varphi_k : S_k \to S_k$, $1 \leqslant k \leqslant n$, astfel încît notînd $a_i^k = a_{\varphi_k(i)}$, $i \in S_k$, să avem $M_k = \{a_0^k, \ldots, a_{k-1}^k\}$ și $a_i^k < a_j^k$ să implice $i < j$. Va rezulta atunci că $M_n = M$ și punem $x_i = a_i^n$.

Pentru $k = 1$, φ_1 este unic determinat. Presupunem deja construită bijecția $\varphi_{k-1} : S_{k-1} \to S_{k-1}$ cu proprietatea indicată și fie $p = \min \{i \in S_{k-1} \mid a_k < a_i^{k-1}\}$. Se consideră atunci aplicația bijectivă

$$\varphi_k : S_k \to S_k, \quad \varphi_k(i) = \begin{cases} i & \text{dacă } i < p, \\ k - 1 & \text{dacă } i = p, \\ i - 1 & \text{dacă } i > p, \end{cases}$$

care are proprietatea cerută.

Din această proprietate rezultă că *orice mulțime ordonată finită are elemente minimale și elemente maximale.*

Funcții de selecție

Așa cum am mai spus, în această carte ne situăm în cadrul utilizării neformalizate a limbajului mulțimilor. Printre construcțiile axiomatice ale teoriei mulțimilor se remarcă axiomatica Zermelo-Fraenkel ([2], [41]), în care se utilizează un singur tip de obiecte, anume mulțimile (notate a, b, x etc.) și un singur tip de relație între mulțimi — apartenența ($\in$). Elementele ca și proprietățile elementelor (prin mulțimile lor de adevăr) sînt asimilabile prin mulțimi. Astfel, $x \in y$ se citește: mulțimea x aparține mulțimii y sau, echivalent, x este un element al lui y. Axiomele sistemului Zermelo-Fraenkel se referă la existența mulțimilor ale căror elemente au o proprietate dată, existența mulțimii vide, existența intersecției, reuniunii, produsului cartezian sau a mulțimii părților, pornind de la mulțimi date. Pentru fundamentarea teoretică a mulțimilor infinite se adaugă două axiome mai speciale:

— **axioma infinitului:** *există o mulțime* a *astfel încît* $\emptyset \in a$ *și* $\forall\, x \in a$, $x \cup \{x\} \in a$. În particular, notînd $s(x) = x \cup \{x\}$ — *succeso-*

rul lui x, rezultă că a conține $\emptyset$, $s(\emptyset)$, $s(s(\emptyset))$ etc. Mulțimea suport a unei dinamici Peano este o astfel de mulțime a.

— **axioma alegerii :** *pentru orice mulțime a, există o funcție $v : \mathbf{p}(a) \setminus \{\emptyset\} \to a$ astfel încît pentru orice submulțime nevidă $x \subset a$ să rezulte $v(x) \in x$.*

Funcția v se numește *funcție de selecție*; se observă că ea selectează din orice parte nevidă a mulțimii arbitrare a un element al acelei părți.

Axioma alegerii are unele consecințe aparent ciudate. Astfel, numai prin utilizarea ei s-au dat exemple de submulțimi nemăsurabile Lebesgue ale intervalului $[0, 1]$.

Matematicienii sînt cu toții de acord asupra viabilității construcțiilor algoritmice în demonstrarea existenței obiectelor matematice, dar nu toți acceptă demonstrațiile existențiale bazate pe axioma alegerii, chiar dacă unele dintre acestea au avut și au importanță deosebită pentru cunoaștere. K. Gödel (1905-1979) a demonstrat că axioma alegerii este independentă de celelalte axiome ale sistemului Zermelo-Fraenkel, deci se pot dezvolta deopotrivă două matematici — una folosind axioma alegerii și alta care nu o acceptă (ca și în cazul coexistenței geometriilor neeuclidiene cu cea euclidiană).

În cele ce urmează, admitem axioma alegerii și pe baza ei vom demonstra un rezultat calitativ important, cuprins în teorema 2.2.

DEFINIȚIA 2.2. Fie X o mulțime nevidă. Ea se numește *infinită* dacă pentru orice $n \in \mathbb{N}$ mulțimea X *nu* este echipotentă cu $S_n = \{x \in \mathbb{N} \mid x < n\}$.

Aceasta se mai numește și *definiția lui Dedekind.*

TEOREMA 2.2. *Fie X o mulțime nevidă. Sînt echivalente următoarele afirmații :*

a) *Mulțimea X este infinită* (în sensul definiției 2.2);

b) *Există o aplicație injectivă de la $\mathbb{N}$ la X;*

c) *Există o parte strictă a lui X echipotentă cu X.*

(Afirmația b) se mai numește și *definiția lui Cantor* a mulțimilor infinite).

Demonstrație. a $\Rightarrow$ b. Din axioma alegerii, există o funcție de selecție

$$v : \mathbf{p}(X) \setminus \{\emptyset\} \to X,$$

astfel încît pentru orice parte nevidă $A \subset X$ să avem $v(A) \in A$. Să considerăm acum funcția

$$\varphi : \mathbf{p}(X) \to \mathbf{p}(X), \quad \varphi(A) = \begin{cases} \emptyset & \text{dacă } A = \emptyset, \\ A \setminus \{v(A)\} & \text{dacă } A \neq \emptyset. \end{cases}$$

Tripletul $(\mathbf{p}(X), \psi)_X$ constituie o dinamică cu inițializare și, conform teoremei 1.1, există și este unic un morfism de dinamici cu inițializare $\varphi : (\mathbf{N}, s)_0 \to (\mathbf{p}(X)_X, \psi)_X$, adică o aplicație

$$\varphi : \mathbf{N} \to \mathbf{p}(X) \text{ astfel incit } \psi \circ \varphi = \varphi \circ s \text{ și } \varphi(0) = X.$$

Pentru orice $n \in \mathbf{N}$, in cazul cind $\varphi(m) \neq \emptyset$ pentru $m \in S_n$, vom nota $P_n = v(\varphi(S_n))$. Evident, $P_0 = \emptyset$. Vom demonstra acum lema următoare.

LEMĂ. *Fie* $n \in \mathbf{N}$ *astfel încît* $\forall\, m \in S_n$, $\varphi(m) \neq \emptyset$. *Atunci* $P_n = X \setminus \varphi(n)$.

Demonstrație. Procedăm prin inducție după n. Dacă $n = 0$, atunci $P_0 = \emptyset$ și $\varphi(0) = X$; evident, $P_0 = X \setminus \varphi(0)$.

Presupunem afirmația adevărată pentru n și, în plus, presupunem că $\forall\, m \in S_{s(n)}$, $\varphi(m) \neq \emptyset$. Deoarece $S_n \subset S_{s(n)}$, rezultă că $\forall\, m \in S_n$, $\varphi(m) \neq \emptyset$, deci folosind ipoteza de inducție, $P_n = X \setminus \varphi(n)$. Apoi, $n \in S_{s(n)}$, deci $\varphi(n) \neq \emptyset$. Atunci $\psi(\varphi(n)) = \varphi(n) \setminus \{v(\varphi(n))\}$, conform însăși definiției aplicației ψ. Avem de arătat că $P_{s(n)} = X \setminus \varphi(s(n))$. Dar $P_{s(n)} = v(\varphi(S_{s(n)})) = v(\varphi(S_n \cup \{n\})) = v(\varphi(S_n) \cup \{\varphi(n)\}) = v(\varphi(S_n)) \cup \{v(\varphi(n))\} = P_n \cup \{v(\varphi(n))\}$. Pe de altă parte, $\varphi(s(n)) = \psi(\varphi(n)) = \varphi(n) \setminus \{v(\varphi(n))\}$ și atunci $X \setminus \varphi(s(n)) = (X \setminus \varphi(n)) \cup \{v(\varphi(n))\} = P_n \cup \{v(\varphi(n))\}$. În concluzie, $P_{s(n)} = X \setminus \varphi(s(n))$ și lema este demonstrată.

Demonstrăm acum afirmația următoare.

(*) *Pentru orice* $m, n \in \mathbf{N}$, *astfel încît* $\varphi(m) \neq \emptyset$, $\varphi(n) \neq \emptyset$ *și* $v(\varphi(m)) = v(\varphi(n))$, *rezultă* $m = n$.

Într-adevăr, dacă $m \leqslant n$ (cazul $n \leqslant m$ se tratează în mod similar), atunci din ipoteza că $v(\varphi(m)) = v(\varphi(n))$ rezultă $v(\varphi(m)) \in \varphi(n)$, deoarece v este funcție de selecție. Conform lemei rezultă $v(\varphi(m)) \notin P_n$, deci $m \notin S_n$ [căci dacă $m \notin S_n$, atunci $v(\varphi(m)) \in v(\varphi(S_n)) = P_n$]. Așadar, $m \leqslant n$ și $m \notin S_n$, deci neapărat $m = n$.

În fine, demonstrăm și afirmația următoare:

(**) *Pentru oricе* $n \in \mathbf{N}$ *avem* $\varphi(n) \neq \emptyset$.

Într-adevăr, în caz contrar, fie $p = \min\{n \in \mathbf{N} \mid \varphi(n) \neq \emptyset\}$. Rezultă că $\forall\, m \in S_p$ avem $\varphi(m) \neq \emptyset$, deci considerînd restricția $\varphi \mid S_p : S_p \to \mathbf{p}(X) \setminus \{\emptyset\}$, aplicația compusă $v \circ (\varphi \mid S_p) : S_p \to X$ este injectivă (conform afirmației (*)). În plus, $v(\varphi(S_p)) = P_p = X \setminus \varphi(p)$, conform lemei; cum $\varphi(p) = \emptyset$, rezultă $v(\varphi(S_p)) = X$, deci aplicația $v \circ (\varphi \mid S_p)$ este și surjectivă. Ar rezulta că $X \sim S_p$, ceea ce contravine ipotezei a) că mulțimea X este infinită. Am demonstrat astfel afirmația (**).

Rezumînd, am dovedit că aplicația compusă

$$v \circ \varphi : \mathbb{N} \to \mathcal{P}(X) \setminus \{0\} \to X$$

este injectivă (aplicînd din nou afirmația (*)) și astfel implicația $a \Rightarrow b$ este complet demonstrată.

b $\Rightarrow$ c. Presupunem că există o aplicație injectivă $f : \mathbb{N} \to X$. Considerăm $Y = (X \setminus f(\mathbb{N})) \cup f(s(\mathbb{N}))$. Avem $Y \subset X$ și deoarece $f(0) \notin Y$ rezultă $Y \subsetneq X$. Apoi, $\mathbb{N} \sim s(\mathbb{N})$, deci $f(\mathbb{N}) \sim f(s(\mathbb{N}))$ și prin urmare

$$X = [(X \setminus f(\mathbb{N})) \cup f(\mathbb{N})] \sim [(X \setminus f(\mathbb{N})) \cup f(s(\mathbb{N}))] = Y.$$

c $\Rightarrow$ a. Presupunem că ar exista o parte strictă Y a lui X echipotentă cu X. Dacă prin absurd mulțimea X ar fi finită, ar exista $n \in \mathbb{N}$ și o aplicație bijectivă $g : X \to S_n$. Atunci $g(Y)$ ar fi o parte strictă a lui S_n, echipotentă cu S_n, ceea ce contravine teoremei 2.1.

Alte proprietăți ale mulțimilor finite (consecințe ale teoremei 2.2.).

1) *Dacă $f : M_1 \to M_2$ este o aplicație injectivă și M_2 este o mulțime finită, atunci mulțimea M_1 este finită.*

Demonstrație. Dacă M_1 ar fi infinită, atunci, conform teoremei 2.2, ar exista o parte $P \subsetneq M_1$ astfel încît $P \sim M_1$. Deoarece f este injectivă, avem $f(P) \sim f(M_1)$ și $f(P) \subsetneq f(M_1)$. Atunci, $M_2 = (M_2 \setminus f(M_1)) \cup f(M_1) \sim (M_2 \setminus f(M_1)) \cup f(P) \subsetneq M_2$, de unde M_2 ar rezulta infinită, ceea ce este absurd. ∎

2) *Fie M o mulțime finită și o aplicație $\varphi : M \to M$. Atunci φ este injectivă, dacă și numai dacă φ este surjectivă (principiul lui Dirichlet).*

Demonstrație. Într-adevăr, dacă φ este injectivă, atunci $M \sim \varphi(M)$ și cum $\varphi(M) \subset M$, rezultă $\varphi(M) = M$ (căci dacă M este finită, $M' \subset M$ și $M' \sim M$, atunci $M' = M$). Prin urmare φ este surjectivă. Pe de altă parte, în ipoteza că φ este surjectivă, rezultă că există o aplicație injectivă $\psi : M \to M$ (deci bijectivă conform primei părți a demonstrației), astfel încît $\varphi \circ \psi = 1_M$. Atunci $\varphi = \psi^{-1}$ va fi bijectivă. ∎

Observație. O versiune a principiului lui Dirichlet este următoarea : *dacă m obiecte sînt introduse în n cutii, atunci există o cutie care conține cel puțin* $\left[\frac{m-1}{n}\right] + 1$ *obiecte.*

Într-adevăr numărul $k = \left[\frac{m-1}{n}\right]$ este întreg și $k \leqslant \frac{m-1}{n} < k + 1$. Dacă am avea exact $k \cdot n$ obiecte, atunci se pot pune cîte k obiecte în fiecare cutie. Deoarece există m obiecte și $m > nk$, atunci există o cutie care conține cel puțin $k + 1$ obiecte.

De exemplu, într-un grup de 2000 de oameni există cel puțin $1 + \left[\frac{1999}{365}\right] = 6$ oameni care au aceeași zi de naștere.

O altă versiune, de această dată infinitistă, este următoarea: *dacă o infinitate de obiecte se află într-un număr finit de cutii, atunci cel puțin o cutie conține o infinitate de obiecte.*

3) *Dacă* $(T, \leqslant)$ *este o mulțime liniar ordonată, atunci, pentru orice parte finită nevidă* $F \subset T$, *există* $\max F$ *și* $\min F$.

Demonstrație. Arătăm că există $\max F$ (similar se va proceda pentru $\min F$). În caz contrar, pentru orice $x \in F$ mulțimea

$$M_x = \{y \in F \mid y > x\}$$

ar fi nevidă (căci dacă $M_x = \emptyset$, atunci $\forall\, y \in F,\ y \leqslant x$ și $x = \max F$). Considerăm aplicația

$$u : F \to \mathbf{p}(F) \setminus \{\emptyset\},\ x \mapsto M_x$$

și fie

$$v : \mathbf{p}(F) \setminus \{\emptyset\} \to F,\ A \mapsto v(A) \in A$$

o funcție de selecție din axioma alegerii. Să punem $\varphi = v \circ u$. Pentru orice $x \in F$ avem $\varphi(x) = v(u(x)) = v(M_x) \in M_x$, deci $x < \varphi(x)$. Pe de altă parte, mulțimea F este nevidă și fie $x_0 \in F$. Considerăm atunci dinamica $(F, \varphi)_{x_0}$ cu inițializare. Conform teoremei 1.1 de inițialitate, există și este unic un morfism de dinamici $f : (\mathbb{N}, s)_0 \to (F, \varphi)_{x_0}$. Prin inducție după n vom dovedi afirmația următoare:

(*) *Pentru orice* $m, n \in \mathbb{N}$, $m < n$, *avem* $f(m) < f(n)$.

Într-adevăr, pentru $n = 0$ afirmația este evidentă; presupunem afirmația (*) adevărată pentru n și o demonstrăm pentru $s(n) = n + 1$. Fie $m \in \mathbb{N}$, $m < s(n)$. Atunci sau $m = n$ și, în acest caz, $f(m) = f(n) < \varphi(f(n)) = f(s(n))$ sau $m < n$ și, conform ipotezei de inducție, $f(m) < f(n) < \varphi(f(n)) = f(s(n))$. Așadar, aplicația $f : \mathbb{N} \to F$ este strict crescătoare și, în particular, este injectivă. Conform teoremei 2.2, mulțimea F ar rezulta infinită, ceea ce este absurd. ■

Ca o consecință a proprietății 3) rezultă că *o parte nevidă a mulțimii* $\mathbb{N}$ *este finită, dacă și numai dacă este majorată.*

Am demonstrat (proprietatea 10 de la p. 83) că orice mulțime ordonată finită are elemente maximale (și minimale). Iată o caracterizare a mulțimilor finite, datorată lui Tarski.

4) *O mulțime* M *este finită, dacă și numai dacă orice parte nevidă a lui* $\mathbf{p}(M)$ *are element maximal relativ la incluziune.*

Dacă M este finită, atunci $\mathbf{p}(M)$ este finită și orice parte nevidă a ei are element maximal. Reciproc, dacă prin absurd M ar fi infinită, atunci mulțimea părților finite ale lui M ar fi o parte nevidă a lui $\mathbf{p}(M)$ care nu are element maximal. ∎

5) *Fie M și N două mulțimi finite și $\varphi : M \to N$ o aplicație injectivă. Dacă M și N au același număr de elemente, atunci φ este bijectivă.*

Demonstrație. Avem $M \sim \varphi(M)$. Deoarece $\varphi(M) \subset N$, iar $\varphi(M)$ și N au același număr de elemente, rezultă că $\varphi(M) = N$, deci φ este surjectivă. ∎

Ca aplicație stabilim următorul rezultat util.

LEMA (*chinezească*). *Fie $n_1, \ldots, n_k$ numere întregi $\geqslant 2$, prime două câte două. Atunci, pentru orice $a_1, \ldots, a_k \in \mathbb{Z}$, există și este unic $x \in S_n$, $n = n_1 \ldots n_k$, astfel încît $x - a_i$ să fie divizibil cu n_i pentru orice $1 \leqslant i \leqslant k$.*

Demonstrație. Considerăm următoarea mulțime finită

$$C = \{(c_1, \ldots, c_k) \in \mathbb{Z}^k \mid 0 \leqslant c_i < n_i, 1 \leqslant i \leqslant k\},$$

având $n = n_1 \ldots n_k$ elemente. Funcția

$$\varphi : S_n \to C, x \mapsto (r_1, \ldots, r_k),$$

unde r_i este restul împărțirii lui x cu n_i, $1 \leqslant i \leqslant k$, este injectivă. Conform proprietății 5, ea rezultă și surjectivă. Luînd $(c_1, \ldots, c_k) \in C$, unde c_i este restul împărțirii lui a_i cu n_i, $1 \leqslant i \leqslant k$, există (și este unic) $x \in S_n$ astfel încît $\varphi(x) = (c_1, \ldots, c_k)$, adică x și a_i dau același rest la împărțirea cu n_i, pentru orice $1 \leqslant i \leqslant k$. ∎

§ 2.2. CARDINALITATE

Cardinalul unei mulțimi

În acest paragraf ne vom referi pe scurt la cardinalul unei mulțimi ca măsură a „bogăției în elemente". Relația de echipotență pe universul $\mathcal{U}$ este o relație de echivalență și ca atare mulțimile (din $\mathcal{U}$) pot fi dispuse în clase de echipotență. Clasa unei mulțimi M se numește *cardinalul lui M* și se notează cu $|M|$ (sau card M). Cardinalul oricărei mulțimi finite poate fi identificat cu numărul ei de elemente.

Fie $\aleph_0 = |\mathbb{N}|$, cardinalul mulțimii $\mathbb{N}$, numit *alef zero* sau *puterea numărabilului*. Reamintim că mulțimile echipotente cu $\mathbb{N}$ se numesc *mulțimi numărabile*. Cardinalul $|\mathbb{R}|$ al mulțimii numerelor reale se mai numește *puterea continuului*.

Dacă $m_1 = |M_1|$, $m_2 = |M_2|$ sînt cardinalele a două mulțimi oarecare, atunci se definesc:

— $m_1 = m_2 \leftrightarrow M_1 \sim M_2$;
— $m_1 \leqslant m_2 \leftrightarrow$ există o aplicație injectivă de la M_1 la M_2;
— $m_1 + m_2 = |M_1 + M_2|$;
— $m_1 m_2 = |M_1 \times M_2|$;
— $m_2^{m_1} = |M_2^{M_1}|$; în particular, $2^{m_1} = |\mathbb{B}^{M_1}|$.

Funcții caracteristice și mulțimi vagi

Dacă M este o mulțime fixată, atunci pentru orice parte $A \subset M$ se poate defini *funcția ei caracteristică*

$$\chi_A : M \to \mathbb{B}, \quad \chi_A(x) = \begin{cases} 1 \text{ dacă } x \in A, \\ 0 \text{ dacă } x \in M \setminus A. \end{cases}$$

Ordonăm mulțimea $\mathbb{B}$ prin convenția ca $0 < 1$. Se demonstrează imediat că dacă $A, B \subset M$, atunci

— $\chi_A = 0 \leftrightarrow A = \emptyset$; $\chi_A = 1 \leftrightarrow A = M$;
— $\chi_A \leqslant \chi_B \leftrightarrow A \subset B$; $\chi_A = \chi_B \leftrightarrow A = B$;
— $\chi_{A \cap B} = \chi_A \cdot \chi_B = \min(\chi_A, \chi_B)$;
— $\chi_{A \cup B} = \chi_A + \chi_B - \chi_{A \cap B} = \max(\chi_A, \chi_B)$;
— $\chi_{\complement A} = 1 - \chi_A$.

Dacă $\mathbf{p} : M \to \mathbb{B}$ este un predicat (unar) pe M și $A = M_{\mathbf{p}}$ este mulțimea lui de adevăr, atunci este evident că $\chi_A = \mathbf{p}$.

L. Zadeh a introdus noțiunea de mulțime vagă (relativ la M), înlocuind $\mathbb{B}$ cu intervalul închis $[0, 1]$. Mai precis, se numește *M-mulțime vagă* (sau *predicat generalizat* pe M) orice funcție $v : M \to [0, 1]$. Dacă v, v' sînt două M-mulțimi vagi, atunci, prin definiție, $v = v' \leftrightarrow \forall x \in M,\ v(x) = v'(x)$; $v \subset v' \leftrightarrow \forall x \in M,\ v(x) \leqslant v'(x)$; $v \cap v' = \min(v, v')$, $v \cup v' = \max(v, v')$; $\complement v = 1 - v$. Funcția constantă 0 și funcția constantă 1 de la M la $[0, 1]$ sînt M-mulțimile vagi *vidă*, respectiv *totală*. Multe din proprietățile uzuale relativ la intersecție, reuniune, complementară se extind la M-mulțimi vagi și acestea formează o latice, dar nu latice booleană (deoarece în general $v \cap \complement v \neq 0$). Prin considerarea mulțimilor vagi se poate lărgi noțiunea de predicat; anume, o M-mulțime vagă $v : M \to [0, 1]$ poate fi interpretată ca asociind oricărui element $x \in M$ valoarea de adevăr $v(x) \in [0, 1]$, numită și probabilitatea cu care proprietatea v este adevărată pentru elementul x. În acest mod se trece de la predicate $M \to \{0, 1\}$ la predi-

cate $M \to [0,1]$, sau, cum se mai spune, de la logica bivalentă la logica infinit-valentă.

Cardinalul unui dicționar și al mulțimii limbajelor

Pentru orice mulțime M, se poate stabili evident o bijecție

$$\chi : \mathfrak{p}(M) \to \mathbb{B}^M, \ A \mapsto \chi_A,$$

asociind oricărei părți a lui M, funcția ei caracteristică.

Rezultă atunci că $\mathfrak{p}(M) \sim \mathbb{B}^M$, deci

$$|\mathfrak{p}(M)| = 2^{|M|}.$$

Din cursurile standard de analiză matematică se știe că reuniunile numărabile de mulțimi numărabile sînt mulțimi numărabile și că $|\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$. Un fapt remarcabil, lesne de demonstrat și caracteristic mulțimilor infinite, este următorul : dacă M este o mulțime infinită, atunci $\forall\, a \in M$, $|M| = |M \setminus \{a\}|$. De asemenea, conform teoremei 2.2, rezultă că o mulțime M este infinită dacă și numai dacă $\aleph_0 \leqslant |M|$.

LEMĂ. *Avem* $|\mathbb{R}| = 2^{\aleph_0}$.

Demonstrație. Vom arăta că $\mathbb{R} \sim \mathbb{B}^{\mathbb{N}}$ și ca atare $|\mathbb{R}| = 2^{|\mathbb{N}|} = 2^{\aleph_0}$. Pentru aceasta să considerăm aplicațiile următoare :

— bijecția $u : \mathbb{B}^{\mathbb{N}} \to [0,1)$, $x = (x_n)_{n \geqslant 0} \mapsto$ numărul real din intervalul $[0,1)$ scris în baza 2 : $0, x_0, x_1 x_2 \ldots$

— o bijecție $v : [0,1) \to (0,1)$, obținută ținînd cont că mulțimea $M = [0,1)$ este infinită și că $(0,1) = M \setminus \{0\}$;

— bijecția $w : (0,1) \to \mathbb{R}$, $x \mapsto -\operatorname{ctg} \pi x$.

Atunci funcția compusă $w \circ v \circ u : \mathbb{B}^{\mathbb{N}} \to \mathbb{R}$ este bijectivă, deci $\mathbb{R} \sim \mathbb{B}^{\mathbb{N}}$. ∎

Deoarece $\mathbb{B}^{\mathbb{N}} \sim \mathfrak{p}(\mathbb{N})$, așa cum am văzut, rezultă totodată că $\mathbb{R} \sim \mathfrak{p}(\mathbb{N})$.

Observație. Deoarece avem aplicația injectivă de incluziune $i : \mathbb{N} \to \mathbb{R}$, $x \mapsto x$, rezultă $\aleph_0 < 2^{\aleph_0}$.

O problemă celebră este cea a verificării ipotezei continuului, adică a demonstrării faptului că nu există cardinale intermediare între puterea numărabilului și puterea continuului. K. Gödel și P. Cohen au demonstrat în 1964 că ipoteza continuului este independentă de sistemul de axiome Zermelo-Fraenkel.

TEOREMA 2.3. *Pentru orice mulțime finită* A,

$$|A^*| = \aleph_0 \text{ și } |\mathfrak{p}(A^*)| = 2^{\aleph_0}.$$

Demonstrație. Avem $A^* = \bigcup_{n \geqslant 0} A^n$. Dar $A^0 = \{\wedge\}$, $A^1 = A$, $A^2 = A \times A$ etc. și mulțimile A^n, $n \geqslant 0$, sînt mulțimi finite ($|A^n| = |A|^n$), disjuncte două cîte două. Atunci reuniunea lor A^* este o mulțime numărabilă. Există deci o aplicație bijectivă $f : A^* \to \mathbb{N}$, iar aplicația

$$\varphi : \mathbf{p}(A^*) \to \mathbf{p}(\mathbb{N}),\ L \mapsto f(L)$$

va fi de asemenea bijectivă. Ca atare, $\mathbf{p}(A^*) \sim \mathbf{p}(\mathbb{N})$ și ținînd cont că $\mathrm{p}(\mathbb{N}) \sim \mathbb{R}$, rezultă $\mathbf{p}(A^*) \sim \mathbb{R}$, adică $|\mathbf{p}(A^*)| = 2^{\aleph_0}$, conform lemei anterioare. ∎

COROLAR. *Mulțimea* $\mathbb{B}^*$ *a tuturor cuvintelor binare este numărabilă, iar mulțimea* $\mathbf{p}(\mathbb{B}^*)$ *a tuturor limbajelor binare este de puterea continuului.*

§ 2.3. NUMĂRĂRI

Am văzut în § 2.1 cum poate fi evaluat numărul de elemente al anumitor mulțimi finite concrete, inclusiv numărul de pași în execuția unui algoritm sau program prin care se prelucrează un set de date.

Mulțimi de obiecte și mulțimi de numere

O idee majoră în aplicarea matematicii constă în a face ca unor obiecte, simboluri, caractere etc. să le corespundă numere, definite în mod convenabil.

Prezentăm cîteva exemple care ilustrează modul prin care diverse mulțimi de obiecte sînt puse în corespondență cu mulțimi de numere.

Exemple. 1) Fie $M = \{a_1, \ldots, a_m\}$, $N = \{b_1, \ldots, b_n\}$ două mulțimi finite în care ordinea elementelor este fixată. Atunci oricărei relații binare $\rho \in \mathbf{p}(M \times N)$ i se asociază o matrice $[a_{ij}]_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$ de tip $m \times n$ cu coeficienți în $\mathbb{B} = \{0, 1\}$, punînd

$$a_{ij} = \begin{cases} 1 & \text{dacă } a_i \rho b_j, \\ 0 & \text{în caz contrar} \end{cases}$$

De obicei, relațiile între mulțimi finite sînt programate tocmai prin matricile asociate.

2) Fie $A = \{a_1, a_2, \ldots\}$ un alfabet finit sau numărabil. Aplicația

$$\tau : A^* \to \mathbb{B}^*,\ a_{i_1} a_{i_2} \ldots a_{i_k} \mapsto 1^{i_1}\, 0\, 1^{i_2}\, 0 \ldots 1^{i_k}\, 0$$

este o traducere în codul binar a întregului dicționar al lui A. Pentru a verifica aceasta trebuie dovedit că aplicația τ este injectivă: dacă $c = a_{i_1} \ldots a_{i_p}$ și $d = a_{j_1} \ldots a_{j_q}$ sînt două cuvinte din A^* astfel încît $\tau(c) = \tau(d)$, atunci rezultă, evident, $p = q$ și $i_1 = j_1, \ldots, i_p = j_p$, deci $c = d$.

Existența aplicației τ dă încă o explicație a succesului ideii folosirii codului binar, prin posibilitatea de a traduce orice text (scris într-un alfabet finit sau numărabil) într-un text binar bine determinat, cu posibilitate de recuperare (decodificare) a acelui text.

3) Fie $M = \{a_1, \ldots, a_n\}$ o mulțime finită oarecare, $|M| = n$, cu ordinea elementelor fixată. Pentru orice parte $T \subset M$ se poate considera șirul de n biți

$$c = c_1 \ldots c_n, \text{ unde } c_i = \begin{cases} 1 \text{ dacă } a_i \in T \\ 0 \text{ dacă } a_i \notin T \end{cases}, \quad 1 \leqslant i \leqslant n.$$

Aplicația

$$\varphi : \mathfrak{p}(M) \to \mathbb{B}^n, \quad T \mapsto c_1 \ldots c_n$$

astfel definită este bijectivă; se obține astfel o nouă demonstrație pentru faptul că $|\mathfrak{p}(M)| = 2^{|M|}$.

De exemplu, dacă $A = \{a_1, a_2, a_3, a_4\}$, atunci submulțimilor $\emptyset$, $\{a_1, a_2\}$, $\{a_1, a_2, a_4\}$ li se asociază respectiv șirurile de biți 0 0 0 0, 1 1 0 0, 1 0 1 1.

Orice parte $T \subset M$ având r elemente se reprezintă printr-un șir de n biți dintre care r termeni sînt egali cu 1 și $n - r$ egali cu 0. În particular, există C_n^r șiruri de n biți având exact r componente egale cu 1.

$\mathbb{N}$-mulțimi

Fie S o mulțime nevidă care este finită sau numărabilă. Se numește *numărare* a lui S orice aplicație surjectivă $\nu : \mathbb{N} \to S$. O pereche (S, ν) formată dintr-o mulțime S și o numărare pe S se numește $\mathbb{N}$-*mulțime*.

Convenind că $\emptyset$ admite o numărare notată prin 0, se poate considera $\mathbb{N}$-mulțimea $(\emptyset, 0)$.

TEOREMA 2.4. *Orice submulțime infinită $A \subset \mathbb{N}$ admite o numărare bijectivă $\nu : \mathbb{N} \to A$* (numită *numărarea canonică* a lui A).

Demonstrație. Pentru orice $n \in \mathbb{N}$ considerăm aplicația $\sigma_n : S_n \to A$, definită prin

$$\sigma_n(0) = \inf A \, ; \; \sigma_n(k) = \inf (A \setminus \{\sigma(0), \sigma(1), \ldots, \sigma(k-1)\})$$

pentru $1 \leqslant k < n$.

Dacă $S_n \subset S_m$ (adică $n \leqslant m$), atunci $\sigma_m | S_n = \sigma_n$ și definim aplicația bijectivă $\nu : \mathbb{N} \to A$ prin $\nu | S_n = \sigma_n$ pentru orice $n \in \mathbb{N}$. ∎

Reținem totodată că orice submulțime a lui $\mathbb{N}$ este finită sau numărabilă.

COROLAR. *Există o aplicație bijectivă*

$$f : \mathbb{N} \to \mathbb{N}^* = \bigcup_{k \geqslant 0} \mathbb{N}^k.$$

Demonstrație. Fie $p_1 < p_2 < p_3 < \ldots$ șirul numerelor prime. Punem $g(\wedge) = 0$ și pentru orice $(x_1, \ldots, x_k) \in \mathbb{N}^k$,

$$g(x_1, \ldots, x_k) = p_1^{x_1} \ldots p_k^{x_k}.$$

Aplicația $g : \mathbb{N}^* \to \mathbb{N}$ astfel definită este evident injectivă și stabilește o bijecție $h : \mathbb{N}^* \to g(\mathbb{N}^*)$, $x \mapsto g(x)$. Conform teoremei 2.4, există o numărare bijectivă $\nu : \mathbb{N} \to g(\mathbb{N}^*)$ și luăm $f = h^{-1} \circ \nu$.

Aplicația f se numește *numărarea canonică* a dicționarului $\mathbb{N}^*$.

Așadar, orice submulțime infinită a lui $\mathbb{N}$ și dicționarul alfabetului $\mathbb{N}$ sînt $\mathbb{N}$-mulțimi.

Fie acum $A = \{a_1, \ldots, a_n\}$ un alfabet finit cu ordinea literelor fixată. Atunci pe dicționarul A^* se poate introduce *ordinea lexicografică*: dacă $x, y \in A^*$ și dacă prima literă a lui x precede prima literă a lui y, atunci $x < y$; dacă primele litere din x și y coincid, comparăm literele secunde etc.; pentru orice cuvinte $x, y \in A^*$ avem $x < y$, $x = y$ sau $y < x$, deci ordinea lexicografică este liniară. Să considerăm monoidul multiplicativ $(\mathbb{N}, \cdot, 1)$. Conform teoremei 1.7, pentru orice aplicație $\gamma : A \to \mathbb{N}$, există și este unic un morfism de monoizi $\gamma^* : A^* \to \mathbb{N}$, astfel încît $\gamma^* \circ i_A = \gamma$; anume, $\forall\, c = a_{i_1} \ldots a_{i_p} \in A^*$ avem $\gamma^*(c) = \gamma(a_{i_1}) \ldots \gamma(a_{i_p})$. Apoi, $\gamma^*(\wedge) = 1$. Deoarece aplicația γ^* este o prelungire a lui γ, o vom nota în continuare tot cu γ.

Exemplu. Fie $A = \{a, b\}$; $\gamma(a) = 1$, $\gamma(b) = 7$. Atunci pentru cuvîntul $c = abba$ avem $\gamma(c) = 1 \cdot 7 \cdot 7 \cdot 1 = 49$.

Să notăm cu $p_1 < p_2 < p_3 < \ldots$ șirul strict crescător al numerelor prime ($p_1 = 2$, $p_2 = 3$, $p_3 = 5$ etc.). Fiecărui element $a_i \in A$ îi asociem cîte o pondere $r_i \in \mathbb{N}$, $1 \leqslant i \leqslant n$, și considerăm aplicația $\gamma : A \to \mathbb{N}$, $a_i \mapsto p_i^{r_i}$. Atunci aceasta se prelungește la cuvintele din A, adică la o aplicație $\gamma : A^* \to \mathbb{N}$, care este injectivă [dacă $c = a_{i_1} \ldots a_{i_k}$, $d = a_{j_1} \ldots a_{j_l} \in A^*$ și $\gamma(c) = \gamma(d)$, atunci $p_{i_1}^{r_{i_1}} \ldots p_{i_k}^{r_{i_k}} = p_{j_1}^{r_{j_1}} \ldots p_{j_l}^{r_{j_l}}$, deci în mod necesar $k = l$ și $i_1 = j_1, \ldots, i_k = j_k$, deci $c = d$]. Mulțimea A^* se identifică prin submulțimea $\gamma(A^*) \subset \mathbb{N}$ și fiind infinită, conform teoremei 2.4 există o numărare bijectivă $\nu : \mathbb{N} \to A^*$.

Mașini Turing și numărarea lui Gödel

Înainte de a da o definiție riguroasă începem cu cîteva considerații euristice. Fie un dispozitiv abstract care lucrează în timp discret (mulțimea momentelor fiind o submulțime a lui $\mathbb{Z}$) și care are o mulțime finită de stări posibile

$Q = \{q_0, q_1, \ldots, q_m\}$, $m \geqslant 1$ (*alfabetul stărilor interne*),

împreună cu o *bandă*, potențial infinită în ambele direcții, pe care pot fi tipărite atît instrucțiuni, convenabil codificate pentru acel dispozitiv, cît și răspunsuri ale dispozitivului. Presupunem că banda este divizată pe întreaga lungime într-o infinitate de pătrățele numerotate prin

numere întregi (din $\mathbb{Z}$), pe fiecare pătrățel fiind tipărit cîte un singur element dintr-o mulțime finită

$$\mathcal{A} = \{a_0, a_1, \ldots, a_n\} \text{ (\textit{alfabetul intrărilor})}.$$

Se mai presupune de asemenea că există un cap de citire și tipărire, care se deplasează în lungul benzii, astfel că la fiecare moment el se află în dreptul unui pătrățel.

Deoarece instrucțiunile sînt scrise cu un număr finit de simboluri și intrucțiunile sînt în număr finit, toate pătrățelele cu excepția unui număr finit sînt albe (vide). Facem convenția ca într-un pătrățel alb să figureze litera a_0 din alfabetul $\mathcal{A}$; a_0 se mai numește simbolul vid (sau blancul). Așadar, la fiecare moment, pe bandă doar un număr finit de pătrățele sînt tipărite cu alte simboluri decît a_0 și banda poate fi deplasată cu cîte un pătrățel spre dreapta sau spre stînga.

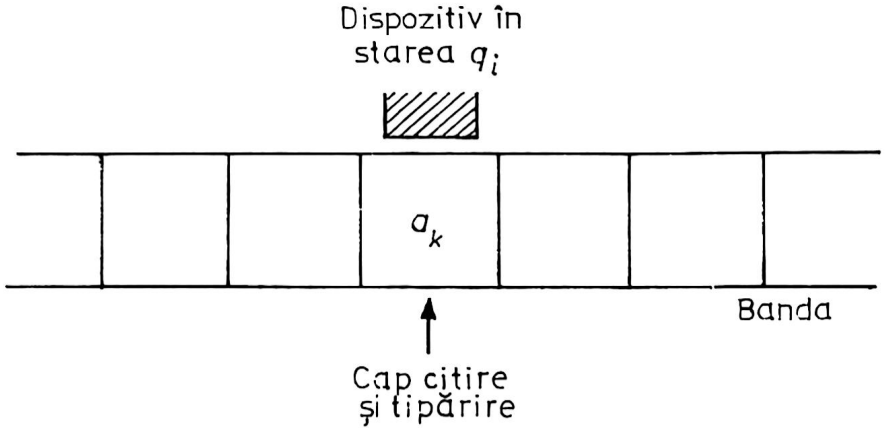


Fig. 2.1

Presupunem că dispozitivul își poate începe lucrul numai dacă se află în starea q_0 din Q (numită starea inițială) și că acțiunea dispozitivului la orice moment este determinată de starea q_i în care se află și de litera a_k care este tipărită pe pătrățelul ce urmează să fie deplasat (fig. 2.1). Presupunem de asemenea că la fiecare moment, răspunsul posibil al dispozitivului este unul din următoarele:

1) se înlocuiește litera a_k de intrare cu o literă a_l și dispozitivul trece din starea q_i în starea q_j;

2) banda este deplasată cu un pătrățel spre dreapta și dispozitivul trece din starea q_i în starea q_j;

3) similar cu 2, dar spre stînga;

4) dispozitivul se oprește.

Un răspuns de tipul 1) al dispozitivului (aflat în starea q_i și primind litera a_k la intrare) este indicat prin 4-uplul (q_i, a_k, a_l, q_j); răspunsurile date de dispozitiv în cazurile 2) și 3) sînt notate (q_i, a_k, D, q_j), respectiv, (q_i, a_k, S, q_j), presupunînd că literele D, S (care

simbolizează dreapta, resp. stînga) nu aparţin alfabetului $\mathcal{A}$. În fine, răspunsul 4), adică oprirea dispozitivului poate fi specificată prin aceea că nu există 4-uple în care primele două componente să fie q_i, a_k.

Aşadar, pentru orice pereche $(q_i, a_k) \in Q \times \mathcal{A}$, există cel mult un 4-uplu care începe cu q_i, a_k. Reţinem că astfel configuraţia dispozitivului la orice moment este determinată de conţinutul benzii (să spunem a_k), de numărul pătrăţelului care urmează să fie deplasat şi de starea internă q_i. Să notăm cu a_{k_n} litera din $\mathcal{A}$ tipărită pe pătrăţelul cu numărul n. Deoarece există doar un număr finit de pătrăţele nealbe, există întregi u, v, nu neapărat unici, astfel încît $k_n = 0$ pentru $n < u$ şi pentru $n > v$. Conţinutul benzii (numit şi configuraţia dispozitivului la momentul considerat) este exprimat prin şirul de simboluri

$$\ldots a_0 a_0 a_{k_u} a_{k_{u+1}} \ldots a_{k_{n-1}} q_i a_{k_n} \ldots a_{k_v} a_0 a_0 \ldots,$$

indicînd explicit că dispozitivul este în starea q_i iar pătrăţelul ce urmează să fie deplasat este cel cu numărul de ordine n. Două astfel de configuraţii, pentru $(q_i, a_k) \in Q \times \mathcal{A}$ fixat şi la un moment dat, diferă doar prin alegerea lui u şi v şi se numesc echivalente.

Pornind de la astfel de consideraţii, A. Turing (1912—1954) a definit conceptul de maşină care îi poartă numele.

DEFINIŢIA 2.3 ([2]). Fie Q şi A două mulţimi finite nevide. Se numeşte *maşină Turing* avînd mulţimea stărilor Q şi mulţimea intrărilor A, orice submulţime finită

$$M \subset Q \times A \times (A \cup \{D, S\}) \times Q, \quad D, S \notin A,$$

cu proprietatea că pentru orice 4-uple

$$(q, a, a', q'), \quad (q, a, a'', q'')$$

care aparţin lui M, rezultă $a' = a''$ şi $q' = q''$.

Fie $M_1 \subset Q_1 \times A_1 \times (A_1 \cup \{D, S\}) \times Q_1$, D, $S \notin A_1$, o altă maşină Turing astfel încît să existe aplicaţii bijective $F : Q \to Q_1$, $G : A \to A_1$ pentru care $\forall (q, a, a', q') \in M$, $(F(q), G(a), G(a'), F(q')) \in M'$. În acest caz, cele două maşini diferă doar prin etichetele care reprezintă stările lor interne, literele de intrare şi esenţialmente ele coincid (sînt izomorfe).

Fixăm o maşină Turing M. Se numeşte *configuraţie instantanee* a lui M, orice şir finit de simboluri de forma

$$w = a_{k_1} a_{k_2} \ldots a_{k_r} q a_{l_1} a_{l_2} \ldots a_{l_s}$$

cu $a_{k_i}, a_{l_j} \in A$ şi $q \in Q$ (nu se exclud cazurile $r = 0$ sau $s = 0$). Aşadar, $w = cqd$, unde $c, d \in A^*$. Două configuraţii instantanee $w = c\,q\,d$

și $w' = c'q'd'$ se spune că sînt *echivalente* dacă $q = q'$, c' se obține din c adăugînd sau eliminînd un număr finit de litere a_0 la stînga, iar d' se obține din d adăugînd sau eliminînd un număr finit de blancuri a_0 la dreapta. Este astfel definită o relație de echivalență (pe mulțimea configurațiilor unei mașini Turing); pentru orice configurație w, clasa sa de echivalență $[w]$ se numește *stare instantanee* a mașinii M, descrisă de w.

Prin definiție, mașina Turing M transformă starea $[w]$ în starea $[w']$ și se scrie

$$[w] \overset{M}{\to} [w']$$

dacă există reprezentanți $w = cqd$, $w' = c'q'd'$ cu $d = a_r d_1$, astfel încît să avem sau

1) $(q, a_r, a_{r'}, q') \in M$ și $c' = c$, $d' = a_{r'} d_1$;

sau

2) $(q, a_r, D, q') \in M$ și $c' = ca_r$, $d' = d_1$;

sau

3) $(q, a_r, S, q') \in M$ și există $a_s \in A$ astfel încît $c = c'a_s$, $d' = a_s d$.

O stare $[w]$, $w = cqd$ se numește *inițială* dacă $q = q_0$; o stare $[w]$, $w = cqa_r d_1$, se numește *terminală* dacă nu există nici un 4-uplu (q, a_r, α, β) care să aparțină lui M.

Se numește *calcul* al mașinii M orice șir finit de stări $[w_0], [w_1], \ldots, [w_n]$, astfel încît $[w_0]$ să fie stare inițială, $[w_n]$ stare finală și $[w_j] \overset{M}{\to} [w_{j+1}]$ pentru $j = 0, 1, \ldots, n-1$. Pentru orice stare $[w]$, există și este unică o stare $[w']$, astfel încît $[w] \overset{M}{\to} [w']$, dar nu există certitudinea că începînd din această stare mașina se va opri (adică va executa un calcul).

Presupunem că mașinile Turing distincte sînt în număr numărabil. Atunci putem fixa alfabete numărabile

$$Q = \{q_0, q_1, q_2, \ldots\}, \quad \mathcal{A} = \{a_0, a_1, a_2, \ldots\},$$

unde q_0 este starea internă inițială iar a_0 blancul, astfel încît orice mașină Turing să utilizeze cîte o submulțime finită a lui Q (conținînd q_0) și cîte o submulțime finită a lui $\mathcal{A}$ (conținînd a_0).

Orice mașină Turing M se poate identifica atunci cu o submulțime finită a lui $Q \times \mathcal{A} \times (\mathcal{A} \cup \{D, S\}) \times Q$. Îi vom asocia un număr natural $\gamma(M)$ bine determinat. Configurațiile care apar în calculele mașinii M pot fi ordonate lexicografic și ca atare mașinii M i se asociază un șir finit bine determinat, notat Σ_M, de cuvinte din dicționarul C^*, unde $C = Q \cup \mathcal{A} \cup \{D, S\}$.

Vom defini numere Gödel pentru diversele simboluri din C punînd :

$\gamma(a_k) = 4k + 5$ pentru orice $k \geqslant 0$;

$\gamma(q_i) = 4i + 7$ pentru orice $i \geqslant 0$; $\gamma(S) = 1$, $\gamma(D) = 3$.

Atunci funcția $\gamma : C \to \mathbb{N}$ astfel definită poate fi extinsă la cuvinte din C^* și apoi șirului finit Σ_M de mai sus. Anume, dacă $p_1 < p_2 < p_3 < \ldots$ este șirul strict crescător al numerelor prime și dacă simbolurile α_i, $1 \leqslant i \leqslant r$, au numerele Gödel $m_i = \gamma(\alpha_i)$, atunci pentru cuvîntul $c = \alpha_1 \ldots \alpha_r$ se pune $\gamma(c) = p_1^{m_1} \ldots p_r^{m_r}$; iar dacă $c_1, \ldots, c_s$ este un șir finit de cuvinte, numărul Gödel al acestui șir este, prin definiție, $p_1^{\gamma(c_1)} \ldots p_s^{\gamma(c_s)}$. *Numărul Gödel* $\gamma(M)$ al mașinii Turing M este tocmai numărul Gödel al șirului Σ_M. Notînd cu $\mathfrak{M}$ mulțimea mașinilor Turing esențialmente distincte, am definit o aplicație

$$\gamma : \mathfrak{M} \to \mathbb{N}, \quad M \mapsto \gamma(M)$$

care este injectivă (dar nu surjectivă). Aplicînd teorema 2.4, este definită o aplicație surjectivă $\nu : \mathbb{N} \to \mathfrak{M}$, numită *numărarea Gödel* a mașinilor Turing.

§ 2.4. STRUCTURI ALGEBRICE PE MULȚIMI FINITE

Monoizi ciclici

Fie $(M, \cdot, 1)$ un monoid notat multiplicativ. Pentru orice $a \in M$ definim aplicația $\varphi_a : M \to M$, $x \mapsto x \cdot a$. Conform teoremei 1.1, există și este unic un morfism de dinamici

$$f_a : (\mathbb{N}, s)_0 \to (M, \varphi_a)_a \text{ astfel încît } f_a(0) = 1.$$

Pentru orice $n \in \mathbb{N}$ avem $f_a(n+1) = f_a(n) \cdot a$ și notînd $f_a(n) = a^n$ rezultă

$$a^0 = 1, \; a^1 = a, \; a^2 = a \cdot a, \; a^{n+1} = a^n \cdot a.$$

Prin inducție după n se verifică ușor că $\forall\, m, n \in \mathbb{N}$, $a^{m+n} = a^m \cdot a^n$.

Monoidul M se numește *ciclic* dacă este generat de un element $a \in M$ (adică $\bar{a} = M$) ; în acest caz,

$$M = \{1, a, a^2, \ldots, a^n, \ldots\}$$

și aplicația $f_a : \mathbb{N} \to M$ este surjectivă ; evident, orice monoid ciclic este comutativ.

Exemple. 1) Monoidul $(\mathbb{N}, +, 0)$ este ciclic, generat de 1; dar monoidul $(\mathbb{N}, \cdot, 1)$ nu este ciclic.

2) Fie X o mulțime finită; monoidul X^* este ciclic, dacă și numai dacă $|X| = 1$.

3) Fie $p \geqslant 1$ întreg. Să considerăm mulțimea $S_p = \{x \in \mathbb{N} \mid x < p\}$ și fie $k \in S_p$. Pentru orice $i, j \in S_p$ definim

$$i \oplus_k j = i + j - u \cdot (p - k),$$

unde u este cel mai mic număr natural astfel încît $u \cdot (p - k) > i + j - p$ (deci, dacă $i + j < p$, atunci $u = 0$). Așadar, $i + j - u \cdot (p - k) \in S_p$, adică $i \oplus_k j \in S_p$. Se obține atunci un monoid finit $(S_p, \oplus_k, 0)$, care este ciclic generat de 1.

În analogie cu teorema 1.5 are loc următorul rezultat.

TEOREMA 2.5. *Orice monoid ciclic este izomorf fie cu* $(\mathbb{N}, +, 0)$, *fie cu* $(S_p, \oplus_k, 0)$ *cu* $0 \leqslant k < p$.

Demonstrație. Fie $(M, \cdot, 1)$ un monoid ciclic, $a \in M$ generatorul său și aplicația surjectivă $f_a : \mathbb{N} \to M$ definită mai sus. Apar două cazuri:

a) *Aplicația* f_a *este injectivă* deci bijectivă; în acest caz, avem $\forall\, m, n \in \mathbb{N}$, $f_a(m + n) = f_a(m) \cdot f_a(n)$ și $f_a(0) = 1$, deci f_a este un izomorfism de monoizi;

b) *Aplicația* f_a *nu este injectivă*; în acest caz, există $p \geqslant 1$ minim, astfel încît să existe $k < p$ cu proprietatea că $a^k = a^p$; prin inducție

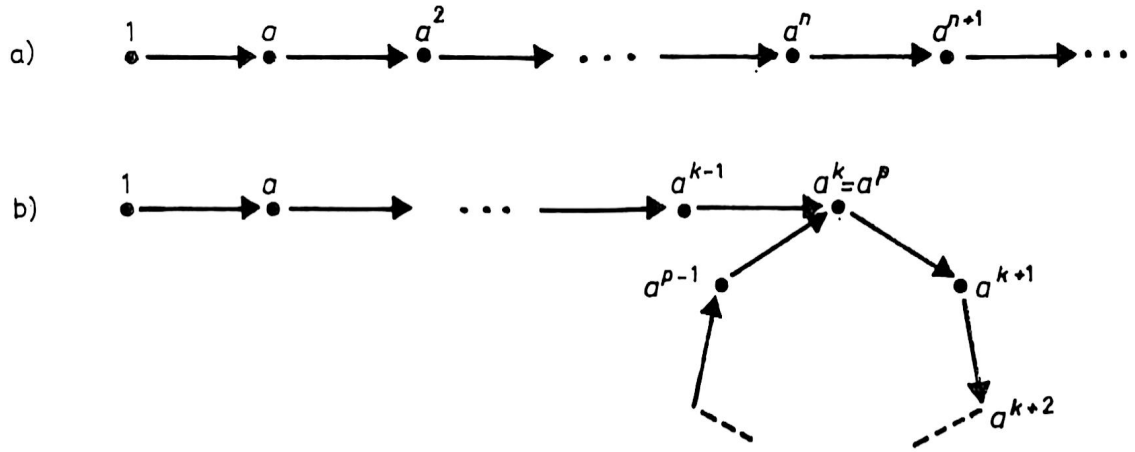


Fig. 2.2

după j se arată ușor că $a^i \cdot a^j = a^{i \oplus_k j}$. Atunci $M = \{1, a, \ldots, a^k, a^{k+1}, \ldots, a^{p-1}\}$ și aplicația

$$g : S_p \to M,\ i \mapsto a^i, \text{ adică } g = f_a \mid S_p$$

stabilește un izomorfism între monoizii $(S_p, \oplus_k, 0)$ și $(M, \cdot, 1)$.

În figura 2.2 sînt redate cele două cazuri; fiecare săgeată semnifică înmulțirea cu a. ∎

Considerăm un monoid $(M, \cdot, 1)$. Un element $a \in M$ se numeşte *idempotent* dacă $a^2 = a$. Elementul neutru al oricărui monoid este evident idempotent. Dacă M este un monoid *finit* şi ciclic generat de a, atunci conform teoremei 2.5 el este izomorf cu un monoid de forma $(S_p, \oplus_k, 0)$ cu $0 \leqslant k < p$. Dacă $k = 0$, atunci singurul idempotent este 1; dar dacă $k \neq 0$, mai există încă un idempotent, anume a^s, unde s este acel unic întreg astfel încît $k \leqslant s < p$ şi $s \vdots p - k$.

Dacă $(S, *)$ este un semigrup finit, atunci, adjuncţionînd un element $e \notin S$ şi punînd $e * e = e$, $e * x = x * e = x$, $\forall\, x \in S$, se obţine un monoid finit $(S', *, e)$, unde $S' = S \cup \{e\}$. Dacă, în plus, $(S, *)$ este ciclic, adică $\exists\, a \in S$ astfel încît $S = \{a^n \mid n \geqslant 1\}$, atunci monoidul $(S', *, e)$ este ciclic generat de a şi, conform teoremei precedente, rezultă că orice semigrup finit ciclic admite exact un idempotent.

În particular, *dacă M este un monoid finit, atunci $\forall\, x \in M$, $\exists\, n \geqslant 1$ întreg astfel ca x^n să fie idempotent.*

Monoizi şi automate finite

Un automat „primeşte" o colecţie de date (numite în mod sugestiv intrări), pe care le „prelucrează" şi apoi „emite" o altă colecţie de date (ieşiri). Notăm cu X mulţimea intrărilor şi cu Y mulţimea ieşirilor. În cursul prelucrării, la fiecare moment automatul se află într-o anumită stare internă. Notăm cu S mulţimea stărilor interne ale automatului. Dinamica automatului poate fi descrisă astfel: oricărei perechi $(x, s) \in X \times S$ îi corespunde un nou element din S, notat $\delta(x, s)$, care reprezintă starea în care trece automatul dacă el primeşte intrarea x şi se află în starea s; pe de altă parte, oricărei perechi $(x, s) \in X \times S$ trebuie să îi corespundă un element bine determinat $\lambda(x, s) \in Y$, anume ieşirea emisă de automat în cazul cînd el primeşte intrarea x şi se află în starea s.

În practică, elementele mulţimilor X, Y, S pot avea o natură foarte diferită (de exemplu, intrările sau ieşirile pot fi tensiuni, impulsuri, sarcini etc.). Conceptul de automat este o extindere sensibilă a celui de sistem intrare-ieşire, definit de § 1.1. De asemenea, un computer digital este un automat foarte complex, avînd o mulţime finită de stări.

Cele spuse anterior, sugerează următoarea definiţie: Se numeşte *automat finit* orice 5-uplu $\mathcal{A} = (X, Y, S, \delta, \lambda)$ în care X, Y, S sînt mulţimi (resp. de intrări, ieşiri şi stări), iar $\delta : X \times S \to S$, $\lambda : X \times S \to Y$ sînt două funcţii. Se presupune în plus că S este o mulţime finită. (În capitolul IV vom da o definiţie formal diferită.)

Funcţia δ se numeşte *dinamica automatului* (sau *tranziţia de stări*), iar λ *funcţia de ieşire.*

Considerînd mulțimea $\mathbb{N}$ ca „mulțime de momente discrete de timp", se pot extinde funcțiile anterioare astfel:

$$\delta : \mathbb{N} \times X \times S \to \mathbb{N} \times S, \quad (t, x, s) \mapsto (t + 1, \delta(x, s));$$

$$\lambda : \mathbb{N} \times X \times S \to \mathbb{N} \times Y, \quad (t, x, s) \mapsto (t, \lambda(x, s)).$$

Așadar, dacă automatul se află la momentul t în starea s și primește intrarea x, atunci el emite simultan (deci tot la momentul t) ieșirea $\lambda(x, s)$ și trece la momentul $t + 1$ în starea $\delta(x, s)$.

De asemenea, dinamica automatului poate fi extinsă la cazul cînd automatul primește succesiuni de litere din X (deci cuvinte din X „citite" de la stînga la dreapta); anume, se definesc inductiv funcțiile $\delta^* : X^* \times S \to S$, $\lambda^* : X^* \times S \to Y$, punînd:

$$\delta^*(\wedge, s) = s \qquad \lambda^*(\wedge, s) = \text{arbitrar}$$

$$\delta^*(wx, s) = \delta(x, \delta^*(w, s)); \qquad \lambda^*(wx, s) = \lambda(x, \delta^*(w, s)),$$

oricare ar fi $w \in X^*$, $x \in X$ și $s \in S$. Așadar, dacă automatul se află în starea s și primește la intrare cuvîntul $c \in X^*$, atunci el va trece în starea $\delta^*(c, s)$ și va emite cuvîntul $\lambda^*(c, s)$ din Y. Dacă prima literă este „citită" la momentul t și dacă c are n litere, atunci automatul va trece în starea $\delta^*(c, s)$ la momentul $t + n$, iar ultima literă a cuvîntului de ieșire $\lambda^*(c, s)$ va fi emisă tot la momentul t.

Remarcăm că dinamica $\delta : X \times S \to S$ determină o funcție $\delta_1 : X \to S^S$, $x \mapsto \delta_1(x)$, unde $\delta_1(x) : S \to S$, $s \mapsto \delta(x, s)$; aplicînd teorema 1.7, δ_1 se extinde la un morfism de monoizi $h : X^* \to S^S$, care induce tocmai pe δ^*, adică $\delta^*(c, s) = h(c)(s)$.

Pe monoidul X^* definim următoarea relație de echivalență ρ: pentru două cuvinte w, $w' \in X^*$ punem

$$w \rho w' \leftrightarrow h(w) = h(w').$$

Așadar, avem $w \rho w'$ dacă și numai dacă $\forall\, s \in S$, $\delta^*(w, s) = \delta^*(w', s)$. Relația ρ este compatibilă cu juxtapunerea de cuvinte (dacă $w \rho w'$, atunci h fiind morfism de monoizi, rezultă că $wu \rho w'u$ și $uw \rho uw'$ pentru orice $u \in X^*$), deci mulțimea-cît X^*/ρ va avea o structură de monoid (punînd $\hat{w}\hat{w}' = \widehat{ww'}$), numit *monoidul automatului* $\mathcal{A}$.

Aplicația $X^*/\rho \to S^S$, $\hat{w} \mapsto h(w)$, este evident bine definită și injectivă. Deoarece S este mulțime finită, rezultă că X^*/ρ este de asemenea finită.

Dacă $\mathcal{A} = (X, Y, S, \delta, \lambda)$ este un automat finit, atunci pentru orice stare $s \in S$ se poate considera *funcția de comportare* (începînd din starea s) $\beta_s : X^* \to Y$, care asociază oricărui cuvînt $c \in X^*$ ultima literă a cuvîntului de ieșire corespunzător $\lambda^*(c, s)$. Automatul $\mathcal{A}$ se numește *redus* dacă : $s \neq s' \Rightarrow \beta_s \neq \beta_{s'}$; în acest caz, toate stările sînt semnificative din punctul de vedere al comportării (nu există stări distincte cu aceeași funcție de comportare). Automatul $\mathcal{A}$ fiind dat și fixînd o stare $s_0 \in S$, se poate construi în mod canonic un automat redus ; anume $\mathcal{A}_r = (X, Y, X^*/\rho, \delta', \lambda')$, unde $\delta' : X \times (X^*/\rho) \to (X^*/\rho)$, $(x, \hat{w}) \mapsto \widehat{wx}$ și $\lambda' : X \times (X^*/\rho) \to Y$, $(x, \hat{w}) \mapsto \beta_{s_0}(wx)$. În teoria automatelor se dă un răspuns complet problemei construirii unui automat redus (obținut restrîngînd mulțimea de stări) cu aceleași proprietăți cu ale unui automat dat.

Observație. Fiind dat un automat finit $\mathcal{A} = (A, B, Q, \delta, \lambda)$ cu A, Q finite și $B = A \cup \{D, S\}$, unde simbolurile D, S nu aparțin lui A, se poate considera o mașină Turing (definiția 2.3) asociată lui $\mathcal{A}$ și realizînd același oficiu ca $\mathcal{A}$; anume $M = \{(q, a, \lambda(q, a), \delta(q, a)) / q \in Q, a \in A\}$.

Cîteva proprietăți ale grupurilor finite

Teoria grupurilor finite este una din cele mai dificile și mai elaborate teorii matematice actuale, cu aplicații în fizică, chimie, cristalografie. În cele ce urmează stabilim doar cîteva proprietăți elementare, utilizate în mod curent ([5], [19], [20], [23], [57]).

1) *Un monoid finit* $(M, \cdot, 1)$ *este grup, dacă și numai dacă* 1 *este singurul idempotent.*

Într-adevăr, dacă M este grup și $a^2 = a$, $a \in M$, atunci, evident, $a = 1$; iar dacă M este monoid finit avînd ca unic idempotent 1, atunci $\forall\, x \in M$ alegem $n \geqslant 1$ astfel ca x^n să fie idempotent, deci $x^n = 1$ și ca atare $x^{n-1} \cdot x = x \cdot x^{n-1} = 1$, deci x admite invers. ■

Ca o aplicație scriem un program care folosește rezultatul anterior. Un masiv T de dimensiuni 100 × 100 conține o tabelă de înmulțire a monoidului $(M, I, 1)$, unde

$$M = \{1, 2, \ldots, N\}, \quad N \leqslant 100 \quad \text{și} \quad I : M \times M \to M, \ (i, j) \mapsto T[i, j].$$

Elementul unitate $1 \in M$ are proprietatea că $T[1, j] = T[j, 1] = j$ pentru orice $j \in M$. Programul atribuie variabilei booleene GROUP valoarea TRUE dacă monoidul $(M, I, 1)$, descris prin masivul T este grup (adică 1 este singurul idempotent) și atribuie valoarea FALSE în caz contrar :

```
begin integer array T[1 : 100, 1 : 100];
integer i, N; Boolean GROUP;
for i = 2 step 1 until N do
if T[i, i] = i then begin GROUP := false; go to F end;
GROUP := true;
F : end
```

2) *Fie* $(G, *, e)$ *un grup şi* $H \subset G$ *o submulţime finită şi stabilă* $(a, b \in H \Rightarrow a * b \in H)$. *Atunci* H *este un subgrup al lui* G.

Pentru demonstraţie, fie $\forall\, x \in H$. Avem $\{e, x, x^2, \ldots\} \subset H$ şi H fiind finită, există numere naturale $i < j$ astfel încît $x^i = x^j$, deci $x^{j-i} = e$. Rezultă că $e \in H$ şi, în plus, $e = x \cdot x^{j-i-1} = x^{j-i-1} \cdot x$, deci există $x^{-1} = x^{j-i-1} \in H$. ∎

Reamintim pe scurt operaţiile cu clase de resturi modulo n. Fie $n \geqslant 2$ un întreg fixat. Relaţia ρ_n de congruenţă modulo n pe mulţimea $\mathbb{Z}$ $(x \rho_n y \leftrightarrow x - y \vdots n)$ este evident o relaţie de echivalenţă. Ea este compatibilă cu adunarea şi înmulţiea $[\forall\, x, x', y, y' \in \mathbb{Z}, x \rho_n x', y \rho_n y' \Rightarrow (x + y)\, \rho_n (x' + y')$ şi $(xy) \rho_n (x'y')]$, deci este compatibilă cu ambele structuri de monoid $(\mathbb{Z}, +, 0)$ şi $(\mathbb{Z}, \cdot, 1)$. Aşadar, mulţimea $\mathbb{Z}_n = \mathbb{Z}/\rho_n$ a claselor de resturi modulo n are, conform teoremei 1.6, două structuri de monoid comutativ $(\mathbb{Z}_n, +, \hat{0})$, $(\mathbb{Z}_n, \cdot, \hat{1})$, punînd

$$x, y \in \mathbb{Z}, \quad \hat{x} + \hat{y} = \widehat{x + y} \text{ şi } \hat{x} \cdot \hat{y} = \widehat{x \cdot y}.$$

3) *Dacă* $n \geqslant 2$ *este un întreg fixat, atunci* $\mathbb{Z}_n = \{\hat{0}, \hat{1}, \ldots, \widehat{n-1}\}$.

Incluziunea „$\supset$" este evidentă; invers, $\forall\, \hat{x} \in \mathbb{Z}_n$, avem $x \in \mathbb{Z}$ şi, conform teoremei împărţirii cu rest, există $q, r \in \mathbb{Z}$ astfel încît $x = nq + r$, $0 \leqslant r < n$, deci $x - r \vdots n$, adică $\hat{x} = \hat{r}$ cu $r \in S_n$. Reţinem că elementele mulţimii S_n constituie un sistem complet de reprezentanţi pentru clase din $\mathbb{Z}_n$. ∎

4) $(\mathbb{Z}_n, +, \cdot, \hat{0}, \hat{1})$ *este un inel comutativ finit cu* n *elemente. Inelul* $\mathbb{Z}_n (n \geqslant 2)$ *este corp, dacă şi numai dacă* n *este prim.*

Axiomele unui inel se verifică imediat. Dacă $\mathbb{Z}_n$ este corp, atunci, în particular, este inel integru, deci n este prim; reciproc, dacă n este prim, atunci inelul $\mathbb{Z}_n$ este integru. Dar orice inel integru finit comutativ A este un corp (căci, dacă $A = \{a_1, a_2, \ldots, a_n\}$, $a_1 = 0$ şi dacă $x \in A \setminus \{0\}$, atunci notînd $xA = \{xa_1, xa_2, \ldots, xa_n\}$ avem $xA \subset A$; apoi, $|xA| = |A|$, deci $xA = A$ şi ca atare $1 \in xA$, deci x admite invers relativ la înmulţire). ∎

În particular, dacă $p \geqslant 2$ este un număr prim, atunci $(\mathbb{Z}_p \setminus \{\hat{0}\}, \cdot, \hat{1})$ este un grup cu $p-1$ elemente.

Observaţie. Fie M o mulţime oarecare; o funcţie $f: \mathbb{Z} \to M$ se numeşte *periodică de perioadă discretă* $n \in \mathbb{Z} (n \geqslant 2)$ dacă $\forall\, x \in \mathbb{Z}$, $f(x + n) = f(x)$. Se poate atunci considera funcţia

$$\tilde{f}: \mathbb{Z}_n \to M, \ \hat{x} \mapsto f(x).$$

Aplicaţia $\tilde{f}$ este bine definită (căci dacă $\hat{x} = \hat{y}$, atunci $x - y \vdots n$, prin urmare $x = y + a \cdot n$ cu $a \in \mathbb{Z}$, deci $f(x) = f(y + a \cdot n) = f(y)$, adică $\tilde{f}(\hat{x}) = \tilde{f}(\hat{y})$). În plus, asocierea

$f \mapsto \tilde{f}$ stabileşte o corespondenţă bijectivă între funcţiile periodice de perioadă discretă $n (n \geqslant 2)$ şi funcţiile oarecare definite pe $\mathbb{Z}_n$; aici se află una din raţiunile considerării mulţimii $\mathbb{Z}_n$.

Un grup $(G, \cdot, 1)$ se numeşte *ciclic*, dacă există $a \in G$ astfel încît $G = \{a^r | r \in \mathbb{Z}\}$. De exemplu, grupul $(\mathbb{Z}, +, 0)$ este ciclic (deşi ca monoid nu este ciclic).

5) *Orice grup ciclic finit G cu $n \geqslant 2$ elemente este izomorf cu grupul* $(\mathbb{Z}_n, +, \hat{0})$.

Într-adevăr, dacă G este ciclic generat de a, atunci aplicaţia $f : \mathbb{Z} \to G$, $r \mapsto a^r$ este un morfism surjectiv de grupuri şi $H = \{r \in \mathbb{Z} | f(r) = 1\} = \operatorname{Ker} f$ este un subgrup al grupului aditiv $\mathbb{Z}$; atunci există $k \in \mathbb{N}$ astfel încît $H = k\mathbb{Z}$; în aceste condiţii aplicaţia $g : \mathbb{Z}_k \to G$, $\hat{x} \mapsto f(x)$ este bine definită şi reprezintă un izomorfism de grupuri; mai mult, deoarece $|G| = n$ rezultă $k = n$. ∎

Printre exemplele importante de grupuri finite se află grupurile de permutări. Dacă X este o mulţime, atunci prin *permutare* a elementelor lui X se înţelege o aplicaţie bijectivă $f : X \to X$; mulţimea acestora se notează σ_X. Atunci $(\sigma_X, \circ, 1_X)$ este un grup, numit *grupul simetric* al mulţimii X. Dacă se ştie că $|X| = n$, atunci $|\sigma_X| = n!$ Dacă $X = \{x_1, \ldots, x_n\}$, atunci orice permutare $f \in \sigma_X$ se poate identifica printr-un tablou

$$f \sim \begin{pmatrix} x_1 \ldots x_n \\ f(x_1) \ldots f(x_n) \end{pmatrix}.$$

A. Cayley (1821-1895) este primul matematician care a introdus noţiunea abstractă de grup şi a arătat că orice grup este izomorf cu un subgrup al grupului său simetric. Mai precis:

6) *Dacă $(G, \cdot, e)$ este un grup, atunci există un morfism injectiv de grupuri $\pi : G \to \sigma_G$.*

Pentru orice $g \in G$ definim $\pi(g) : G \to G$, $x \mapsto g \cdot x$; evident, $\pi(g)$ este o aplicaţie bijectivă. Dacă $\pi(g) = \pi(h)$, atunci $\forall\, x \in G$, $g \cdot x = h \cdot x$, deci $g = h$. Aşadar, aplicaţia π este injectivă. În plus, $\forall\, g, h \in G$, $\pi(g \cdot h)(x) = (g \cdot h)(x) = g \cdot (h \cdot x) = \pi(g)(h \cdot x) = \pi[(g) \circ \pi(h)](x)$ oricare ar fi $x \in G$, deci $\pi(g \cdot h) = \pi(g) \circ \pi(h)$. ∎

Fie $(G, \cdot, 1)$ un grup; un subgrup $H \subset G$ se numeşte *normal* dacă $\forall\, x \in G$ avem $xH = Hx$, adică $\{xh | h \in H\} = \{lx | l \in H\}$. Dacă G este abelian, atunci orice subgrup al lui G este normal.

Demonstrăm acum o proprietate importantă a grupurilor finite, datorată lui Lagrange (1736-1813).

7) *Dacă $H \subset G$ este un subgrup normal al unui grup finit, atunci $|G|$ este divizibil cu $|H|$.*

Pentru demonstraţie, definim pe G relaţia binară ρ punînd pentru $x, y \in G$,

$$x \rho y \leftrightarrow xy^{-1} \in H.$$

Se obține o relație de echivalență pe G, compatibilă cu structura de grup (adică $x\rho x'$, $y\rho y' \Rightarrow (xy)\rho(x'y')$). Atunci mulțimea claselor de echivalență, notată G/H, admite o structură de grup relativ la înmulțirea

$\hat{x} \cdot \hat{y} = \widehat{x \cdot y}$ $(\forall\, x, y \in G)$, cu elementul neutru $\hat{1}$.

Fixăm un sistem complet de reprezentanți S pentru clasele din G/H. Atunci avem o partiție

$$G = \bigcup_{x \in S} \hat{x}.$$

În plus, pentru orice $x \in G$ există o bijecție

$\psi : \hat{x} \to H$, $a \mapsto$ acel unic $h \in H$ astfel încît $a = x \cdot h$, prin urmare $|\hat{x}| = |H|$. În concluzie, $|G| = |S| \cdot |H|$, deci $|G| : |H|$. ∎

Fie $(G, \cdot, 1)$ un grup finit cu g elemente, $g = |G|$. Pentru orice $x \in G$ aplicația $f : \mathbb{Z} \to G$, $r \mapsto x^r$, este morfism de grupuri. Fie $H = \{r \in \mathbb{Z} \mid f(r) = 1\} = \operatorname{Ker} f$, deci H este un subgrup al grupului aditiv $\mathbb{Z}$; atunci există $k \in \mathbb{N}$, $k \geqslant 1$, astfel încît $H = k\mathbb{Z}$. Deoarece aplicația $g : \mathbb{Z}_k \to G$, $\hat{x} \mapsto f(x)$, este un morfism injectiv de grupuri, din proprietatea lui Lagrange rezultă că g este divizibil cu k; în particular, $x^g = 1$. Reținem deci:

8) *Pentru orice grup finit G având g elemente și pentru orice $x \in G$ avem $x^g = 1$.*

Ca aplicație, demonstrăm următorul rezultat important.

TEOREMA 2.6 (*Fermat*). *Fie $p \geqslant 2$ un număr prim. Pentru orice $x \in \mathbb{Z}$ avem $x^p - x \vdots p$.*

Demonstrație. Considerăm grupul $(\mathbb{Z}_p \setminus \{0\}, \cdot, 1)$ având $p - 1$ elemente. Atunci, pentru orice $\hat{x} \in \mathbb{Z}_p$, $\hat{x} \neq \hat{0}$, avem $\hat{x}^{p-1} = \hat{1}$. Prin urmare, $\forall\, \hat{x} \in \mathbb{Z}_p$ avem $\hat{x}^p = \hat{x}$, adică $x^p - x \vdots p$. ∎

Demonstrăm în fine o proprietate care va fi folosită în teorema 2.7. Dacă G este un grup, un element $a \in G$ se spune că este *de ordin k* dacă subgrupul ciclic $\{a^r \mid r \in \mathbb{Z}\}$ este finit, având k elemente; dacă în plus, $|G| = n$, atunci n este divizibil cu k, conform 7.

9) *Fie G un grup abelian finit cu g elemente, presupus neciclic. Atunci, există un divizor h al lui g $(h \neq 1, h \neq g)$ astfel încît $x^h = 1$ pentru orice $x \in G$.*

Pentru demonstrație descompunem $g \in \mathbb{N}$ în produs de numere prime: $g = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ $(p_1 < p_2 < \ldots < p_r)$. Notăm cu k_i' cel mai mare întreg astfel încît grupul G să conțină un element de ordin $p_i^{k_i'}$, deci $k_i' \leqslant k_i$. Dacă $k_i' = k_i$ pentru orice i și $y_1, \ldots, y_r$ sînt elemente din G de ordin $p_1^{k_1}, \ldots, p_r^{k_r}$, cum G este abelian, rezultă că elementul $y = y_1 \ldots y_r$ are ordinul $p_1^{k_1} \ldots p_r^{k_r}$ și G ar rezulta

ciclic, caz exclus. Rezultă în mod necesar că există i astfel încît $k_i' < k_i$, deci $h = \prod_{i=1}^{r} p_i^{k_i'}$ este un divizor al lui g ($h \neq 1, h \neq g$). Fie $\forall\, x \in G$ și $p_1^{c_1} \ldots p_r^{c_r}$ ordinul elementului x. Punînd $n_i = \prod_{j \neq i} p_j^{c_j}$, rezultă că elementul $y_i = x^{n_i}$ are ordinul $p_i^{c_i}$ și de aceea $c_i \leqslant k_i'$. Așadar, ordinul lui x divide h, deci $x^h = 1$. ∎

Corpuri finite

Fie $(K, +, \cdot, 0, 1)$ un corp finit, avînd $n \geqslant 2$ elemente ($1 \neq 0$). Aplicația $f : \mathbb{Z} \to K$, $k \mapsto k \cdot 1$ este un morfism de inele. Există $p \geqslant 2$ minim astfel încît $p \cdot 1 = 0$ [considerînd subgrupul aditiv $H = \{k \in \mathbb{Z} \mid k \cdot 1 = 0\} = \operatorname{Ker} f$, există $p \in \mathbb{Z}$, $p \geqslant 0$ minim, astfel încît $H = p\mathbb{Z}$ și nu putem avea nici $p = 1$, căci ar rezulta $H = \mathbb{Z}$ și $1 = 0$, nici $p = 0$, căci ar rezulta f injectivă, ceea ce contravine finitudinii lui K]. Atunci, numărul p rezultă prim și se numește *caracteristica* lui K; în plus, rezultă un morfism injectiv de inele (de fapt, corpuri)

$$\tilde{f} : \mathbb{Z}_p \to K, \quad \hat{x} \mapsto f(x) = x \cdot 1.$$

Exemple. 1) Corpul $\mathbb{Z}_2$ are caracteristica 2, iar $\mathbb{Z}_7$ are caracteristica 7.

2) Orice corp finit K are o caracteristică p ($p \geqslant 2$ prim) și conține un subcorp izomorf cu $\mathbb{Z}_p$. În acest caz, pentru orice $x, y \in K$ avem $p \cdot x = 0$ și $(x + y)^p = x^p + y^p$. Într-adevăr, $p \cdot x = p(1 \cdot x) = (p \cdot 1)x = 0 \cdot x = 0$; apoi, cum p este prim avem $C_p^k \vdots p$ pentru $1 \leqslant k \leqslant p - 1$, deci $C_n^k \cdot a = 0$, $\forall\, a \in K$, $1 \leqslant k \leqslant p - 1$ și aplicînd formula binomului lui Newton, rezultă $(x + y)^p = x^p + y^p$.

Un rezultat profund, pe care nu îl demonstrăm aici, afirmă că *orice corp finit este comutativ* (teorema lui Wedderburn).

Fie K un corp finit : am văzut că există un corp L izomorf cu $\mathbb{Z}_p$ ($p \geqslant 2$ prim) astfel încît $L \subset K$. Atunci K este un spațiu vectorial peste L de dimensiune finită (de exemplu m) și alegînd o bază $\{e_1, \ldots, e_m\}$ a lui K peste L, există aplicația bijectivă

$$g : L^m \to K, \quad (u_1, \ldots, u_m) \mapsto \sum_{i=1}^{m} u_i e_i,$$

ceea ce arată că $|K| = |L^m| = |L|^m = p^m$. Așadar, *un corp finit are un număr de elemente egal cu o putere naturală a unui număr prim.* (De exemplu, nu există corpuri avînd șase elemente).

Corpurile finite se mai numesc *cîmpuri Galois* (1811—1832). Pentru fiecare $p \geqslant 2$ prim și pentru orice întreg $n \geqslant 1$ se notează cu $\mathrm{GF}(p^n)$ un corp finit cu p^n elemente. Dacă $x \in \mathrm{GF}(p^n)$, atunci $x^q = x$, unde $q = p^n$ [Într-adevăr, grupul multiplicativ al corpului are $q - 1$

elemente, deci $x^{q-1} = 1$ pentru orice $x \in GF(p^n)$, $x \neq 0$.] În plus, dacă $x_1, \ldots, x_q$ sînt elementele corpului $GF(p^n)$, atunci în mod evident $x^q - x = (x - x_1) \ldots (x - x_q)$.

Exemplu. Indicăm un corp cu patru elemente $GF(2^2)$ dînd tabelele de adunare și înmulțire pentru elementele sale, notate 0, 1, $j, j+1$.

+	0	1	j	$j+1$
0	0	1	j	$j+1$
1	1	0	$j+1$	j
j	j	$j+1$	0	1
$j+1$	$j+1$	j	1	0

·	0	1	j	$j+1$
0	0	0	0	0
1	0	1	j	$j+1$
j	0	j	$j+1$	1
$j+1$	0	$j+1$	1	j

Reamintim că dacă K este un corp comutativ, un polinom neconstant $P \in K[X]$ cu coeficienți în K se numește *reductibil* peste K dacă există polinoame neconstante $Q_1, Q_2 \in K[X]$ astfel încît $P = Q_1 \cdot Q_2$ și *ireductibil* (peste K) în caz contrar.

Exemple. 1) Polinomul $X^2 + 1$ este ireductibil peste $\mathbb{R}$, dar nu și peste $\mathbb{C}$. În mod similar, polinomul $X^2 + X + 1$ este ireductibil peste $\mathbb{Z}_2$; dar $X^2 + X + 1$ este reductibil peste $\mathbb{Z}_3$ pentru că $X^2 + X + 1 = (X + 2)^2$.

2) Prin calcul direct se poate arăta că polinoamele ireductibile peste $\mathbb{Z}_2$ de grad $\leqslant 4$ sînt: X, $X+1$, X^2+X+1, X^3+X+1, X^3+X^2+1, X^4+X+1, X^4+X^3+1, $X^4+X^3+X^2+X+1$.

3) Conform teoremei fundamentale a algebrei, singurele polinoame ireductibile peste $\mathbb{C}$ sînt polinoamele de gradul întîi, iar peste $\mathbb{R}$ sînt ireductibile exact polinoamele de gradul întîi și polinoamele de gradul al doilea $X^2 + aX + b$ cu $a^2 - 4b < 0$.

Un rol deosebit îl au în teoria codificărilor polinoamele cu coeficienți în $\mathbb{Z}_2$. Fie $\mathbb{B}$ codul binar, identificat cu $\mathbb{Z}_2$. Orice aplicație injectivă $\gamma : \mathbb{B}^m \to B^n$ $(m \leqslant n)$ se numește o (m, n)-*codificare*.

Să fixăm un întreg $n \geqslant 1$ și un polinom $Q = \alpha_0 + \alpha_1 X + \ldots + \alpha_p X^p$, $Q \in \mathbb{Z}_2[X]$ cu $\alpha_0 \neq 0$ și $\alpha_p \neq 0$. Considerăm aplicația

$$\gamma : \mathbb{B}^n \to \mathbb{B}^{n+p}$$

definită astfel: fie $\forall a = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{B}^n$ fixat și polinomul asociat $P_a = a_0 + a_1 X + \ldots + a_{n-1} X^n$; se consideră polinomul-produs $P_a \cdot Q$, de grad $n + p - 1$, $P_a Q = a_0\alpha_0 + (a_0\alpha_1 + a_1\alpha_0)X + (a_0\alpha_2 + a_1\alpha_1 + a_2\alpha_0)X^2 + \ldots + a_{n-1}\alpha_p X^{n+p-1}$ din $\mathbb{Z}_2[X]$ și se pune $\gamma(a) = (a_0\alpha_0, a_0\alpha_1 + a_1\alpha_0, \ldots, a_{n-1}\alpha_p)$.

Se verifică imediat că aplicația γ este injectivă, deci este o $(n, n+p)$-codificare (cu „cheia" Q).

Exemplu. Luăm $Q = 1 + X^3 + X^4$ și $n = 2$. Atunci aplicația $\gamma : \mathbb{B}^2 \to \mathbb{B}^6$ este definită prin:

$\gamma(0, 0) = (0, 0, 0, 0, 0, 0)$; $\gamma(0, 1) = (0, 1, 0, 0, 1, 1)$;

$\gamma(1, 0) = (1, 0, 0, 1, 1, 0)$; $\gamma(1, 1) = (1, 1, 0, 1, 0, 1)$.

TEOREMA 2.7. *Fie $n \geq 1$ întreg, $p \geq 2$ prim și $K = \mathrm{GF}(p^n)$ un cîmp Galois care conține $L = \mathbb{Z}_p$. Atunci, există un element $c \in K$, rădăcină a unui polinom ireductibil din $L[X]$, astfel încît $1, c, \ldots, c^{n-1}$ să formeze o bază pentru spațiul vectorial K* peste L.

(Așadar, elementele lui $\mathrm{GF}(p^n)$ pot fi scrise sub forma $a_0 + a_1 c + \ldots + a_{m-1} c^{m-1}$ cu $a_i \in \mathbb{Z}_p$; un element c îndeplinind condițiile din enunț este numit *element primitiv* al lui $\mathrm{GF}(p^n)$).

Demonstrație. Conform ipotezei, $\dim_L K = n$. Arătăm că *grupul multiplicativ $G = K \setminus \{0\}$ al lui K este ciclic.* [Într-adevăr, acest grup are $q - 1$ elemente, unde $q = p^n$ și dacă nu ar fi ciclic, atunci, conform proprietății 9 de la p. 104, ar exista un întreg $r \geq 2$, $r \neq q - 1$, care divide $q - 1$ și astfel încît $x^r = 1$ pentru orice $x \in G$. Atunci, $\prod_{x_i \in G} (x - x_i)$ divide $x^r - 1$ cu $r < q - 1$, ceea ce este imposibil deoarece polinomul are grad mai mare decît r.] Există deci $c \in G$ astfel încît $G = \{c^n \mid n \in \mathbb{Z}\}$. Atunci *cel mai mic subcorp al lui K care conține L și c este K.*

Elementele $1, c, \ldots, c^n$ sînt în număr de $n + 1$ și cum $\dim_L K = n$, rezultă că ele sînt liniar independente peste L, deci c este rădăcina unui polinom $S \in \mathbb{Z}_2[X]$ de grad *minim* $s \leq n$. Prin urmare S este ireductibil (altminteri c ar fi rădăcina unui polinom de grad mai mic). În plus, $1, c, \ldots, c^{s-1}$ formează un sistem de generatori pentru K (ca spațiu vectorial peste L), deci $\dim_L K \leq s$; într-adevăr, este suficient să observăm că pentru orice polinom $P \in L[X]$, împărțind P cu S există $Q, R \in L[X]$ astfel încît $P = S \cdot Q + R$ cu $\mathrm{gr}\, R < s$, deci $P(c) = R(c)$; în consecință, rezultă $s = n$ și, în plus, $1, c, \ldots, c^{n-1}$ constituie o bază pentru K peste L. ∎

Exemple. 1) Cîmpul Galois $\mathrm{GF}(2^2)$ are un element primitiv α astfel încît $\alpha^3 = 1$, $\alpha \neq 1$. Tablele de adunare și înmulțire pot fi date astfel:

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

·	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

2) Polinomul $X^4 + X^3 + 1$ este ireductibil peste $\mathbb{Z}_2$. Să considerăm corpul $K = \mathrm{GF}(2^4)$ definit prin $K = \mathbb{Z}_2[X]/(X^4 + X^3 + 1)$, adică mulțimea claselor de echivalență de polinoame $P \in \mathbb{Z}_2[X]$, în raport cu relația $P_1 \sim P_2 \leftrightarrow P_1 - P_2 \vdots X^4 + X^3 + 1$. Se verifică ușor că se poate lua $c = \hat{X}$ și că $1, c, \ldots, c^{15}$ formează o bază a lui K peste L.

Presupunem acum $p = 2$ și identificăm $\mathbb{Z}_2$ cu $\mathbb{B}$, codul binar. Conform teoremei 2.7, există $c \in \mathrm{GF}(2^n)$ astfel încît $1, c, \ldots, c^{n-1}$ să fie o bază a lui $\mathrm{GF}(2^n)$ peste $\mathbb{Z}_2$. Atunci, pentru orice $x \in \mathrm{GF}(2^n)$,

există și sînt unice elemente $a_1, \ldots, a_n \in \mathbb{B}$, astfel încît $x = \sum_{i=1}^{n} a_i c^{i-1}$, iar aplicația $GF(2^n) \to \mathbb{B}^n$, $x \mapsto (a_1, \ldots, a_n)$ este bijectivă. Așadar, *elementele lui* $GF(2^n)$ *pot fi identificate într-un mod canonic prin cuvinte binare de* n *biți.*

Reluînd exemplul 2) anterior, avem $n = 4$ și identificările $c = \hat{X} = 0010$, $c^2 = 0100$, $c^3 = 1000$, $c^4 = 1001$, $c^5 = 1011$, $c^6 = 1111$, $c^7 = 0111$, $c^8 = 1110$, $c^9 = 0101$, $c^{10} = 1010$, $c^{11} = 1101$, $c^{12} = 0011$, $c^{13} = 0110$, $c^{14} = 1100$, $c^{15} = 0001$; se organizează astfel $\mathbb{B}^4$ ca un corp $GF(2^2)$.

Observație. Fie A o mulțime finită de obiecte (sau simboluri), $A = \{a_1, \ldots, a_p\}$, cu o ordine fixată a elementelor. Alegem întregul natural n minim astfel încît $2^n \geqslant p$ și apoi adjuncționăm la mulțimea A un număr finit de simboluri convenționale distincte $\beta_{p+1}, \ldots, \beta_{2^n}$. Mulțimea $A' = \{a_1, \ldots, a_p, \beta_{p+1}, \ldots, \beta_{2^n}\}$ are 2^n elemente distincte, deci există o bijecție $h : A' \to S_{2^n}$. Atunci elementelor $h(a)$, $a \in A'$, le vor corespunde elemente bine determinate din $S_{2^n} = \{0, 1, \ldots, 2^n - 1\}$, care admit o reprezentare binară unică de lungime n. Anume $\forall\, x \in S_{2^n}$ există și sînt unice $x_0, x_1, \ldots, x_{n-1} \in \mathbb{B}$ astfel încît $x = \sum_{i=0}^{n-1} x_i 2^i$. Iată deci un mod de a asocia unei mulțimi (finite) de obiecte oarecare, o reprezentare binară a acelor obiecte. Teorema 2.7 permite un mod sistematic, bazat pe exploatarea structurii de corp, de a reprezenta elementele unui cîmp Galois $GF(2^n)$ prin cuvinte binare de lungime n.

CAPITOLUL 3

STRUCTURI ARBORESCENTE ȘI CALCULABILITATE

Introducere

Printre noțiunile de bază ale matematicii discrete se află cea de graf, care modelează diverse tipuri de rețele, circuite electrice sau microelectronice. Grafurile și mai ales structurile arborescente sînt de asemenea utilizate în programare, în studiul transformărilor între registre ca și în descrierea structurii sintactice sau semantice a lanțurilor corecte de cuvinte etc.

Noțiunea de categorie este legată de cea de graf și de realizarea ideii ca odată cu o colecție de obiecte, să fie considerate modalitățile de interconectare a obiectelor respective. De exemplu, odată cu mulțimile sînt considerate aplicațiile de mulțimi, odată cu grupurile — morfismele de grupuri etc. În acest capitol vom prezenta succint conceptele de graf, categorie, arbore etichetat, acesta din urmă fiind strîns legat de unele noțiuni de algebră universală. Desigur, fiecare din acestea fac obiectul unor tratări amănunțite în cărți de specialitate ([13], [39], [56]). Vom introduce de asemenea noțiunea matematică de automat finit, subliniind faptul că automatele și circuitele logice sînt cazuri speciale de sisteme dinamice discrete. În ultimul timp, teoria automatelor a cunoscut o puternică dezvoltare, iar tendința de algebrizare a influențat pozitiv această dezvoltare.

În ultimul paragraf prezentăm conceptul de calculabilitate. Dacă ne gîndim că etimologic „calcul=piatră mică", putem aprecia saltul imens realizat în înțelegerea mecanismelor matematice ale calculului programat, nu neapărat numeric, legate de explicitarea unor seturi de instrucțiuni privind realizarea procedurilor efective.

§ 3.1. GRAFURI ȘI CATEGORII

Grafuri orientate, morfisme de grafuri

Noțiunea de graf are multe surse și puternice motivații.

DEFINIȚIA 3.1. Un *graf orientat* (pe scurt, *graf*) este un 4-uplu

$$G = (V, A, i, t)$$

alcătuit din două mulțimi și două aplicații de mulțimi :

1) mulțimea V *a vîrfurilor* și mulțimea A *a arcelor* ;

2) $i : A \to V$ și $t : A \to V$.

Pentru orice arc $a \in A$, $i(a)$ se numeşte *iniţialul* arcului a, iar $t(a)$ *terminalul* lui a. Se spune că vîrfurile v, v' din V *sînt unite* în graful G printr-un arc $a \in A$ şi se scrie $v \xrightarrow{a} v'$ în cazul cînd $i(a)=v$ şi $t(a) = v'$. Vom nota cu $G(v, v')$ mulţimea tuturor arcelor avînd iniţialul v şi terminalul v', deci

$$G(v, v') = \{a \in A \mid v \xrightarrow{a} v'\}.$$

Uneori vîrfurile mai sînt numite noduri iar arcele — muchii.

Exemple. 1) Fie $V = \{a, b\}$, $A = \{\alpha, \beta, \gamma\}$;

$$i: A \to V, \begin{matrix} \alpha \mapsto a \\ \beta \mapsto a \\ \gamma \mapsto b \end{matrix} \quad \text{şi} \quad t: A \to V, \begin{matrix} \alpha \mapsto a \\ \beta \mapsto b \\ \gamma \mapsto a. \end{matrix}$$

Graful $G = (V, A, i, t)$ astfel definit poate fi vizualizat ca în fig. 3.1.

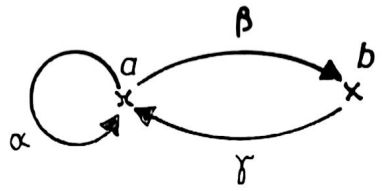


Fig. 3.1.

Iar desenul din fig. 3.2 ilustrează graful $G = (V, A, i, t)$, unde $V = \{v_1, v_2, v_3\}$, $A = \{a_1, a_2, a_3\}$;

$$i: A \to V, \begin{matrix} a_1 \mapsto v_2 \\ a_2 \mapsto v_3 \\ a_3 \mapsto v_3 \end{matrix} \quad \text{şi} \quad t: A \to V, \begin{matrix} a_1 \mapsto v_3 \\ a_2 \mapsto v_3 \\ a_3 \mapsto v_3 \end{matrix}$$

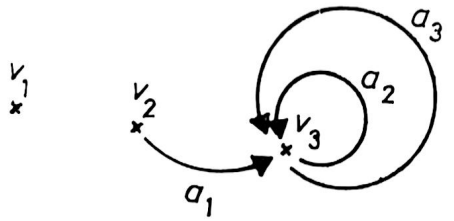


Fig. 3.2

2) Pentru orice graf $G = (V, A, i, t)$ se definesc în mod natural subgrafurile lui G ca fiind grafuri de forma (V', A', i', t'), unde $V' \subset V$, $A' \subset A$, $i(A') \subset V'$, $t(A') \subset V'$ şi $i' = i|A'$, $t' = t|A'$. Dacă $W \subset V$ este o submulţime de vîrfuri în G, atunci *subgraful lui G generat de W* este, prin definiţie, graful $(W, A_W, i|A_W, t|A_W)$, unde $A_W = \{a \in A \mid i(a) \in W$ şi $t(a) \in W\}$.

3) Un exemplu de graf avînd o mulțime infinită de vîrfuri este

$G_\omega = (\mathbb{N}, S, p_1, p_2)$, unde $S = \{(p, p+1) \mid p \in \mathbb{N}\} \subset \mathbb{N}^2$ și $p_1, p_2 : S \to \mathbb{N}$ sînt proiecțiile canonice. Vom nota cu $P_n (n \in \mathbb{N}$ fiind fixat), subgraful lui G_ω generat de $S_n = \{x \in \mathbb{N} \mid x < n\}$. Se poate de asemenea considera pentru orice întreg $n \geqslant 2$ graful finit $Q_n = (\mathbb{Z}_n, T, p_1, p_2)$, unde $T = \{(\hat{k}, \widehat{k+1}) \mid k \in S_n\} \subset \mathbb{Z}_n^2$ iar $p_1, p_2 : T \to \mathbb{N}$ sînt proiecțiile canonice.

Aceste trei grafuri pot fi vizualizate în fig. 3.3.

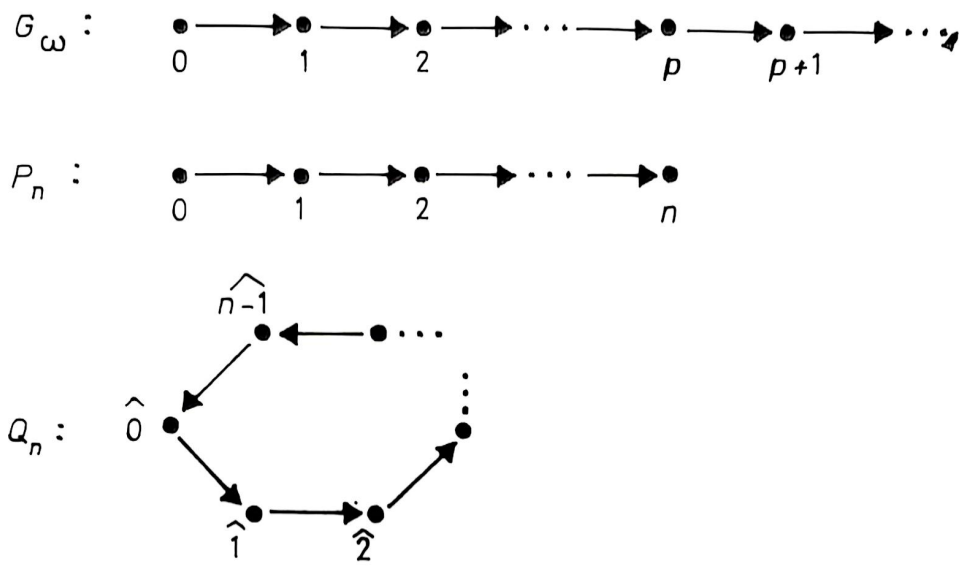


Fig. 3.3

Fie $G = (V, A, i, t)$, $G' = (V', A', i', t')$ două grafuri orientate. Se numește *morfism de grafuri* $h : G \to G'$ de la G la G', orice pereche de aplicații

$$h = (h_V, h_A),$$

unde $h_V : V \to V'$, $h_A : A \to A'$ sînt compatibile cu vîrfurile și arcele, în sensul că $h_V \circ i = i' \circ h_A$ și $h_V \circ t = t' \circ h_A$. Aceasta revine la faptul că

$$\forall\, a \in A \text{ și } v \xrightarrow{a} v', \text{ rezultă } h_V(v) \xrightarrow{h_A(a)} h_V(v').$$

Dacă $G'' = (V'', A'', i'', t'')$ este un alt graf și $k : G' \to G''$ este un morfism de grafuri, atunci se definește în mod natural *morfismul compus* $k \circ h$. Pentru orice graf $G = (V, A, i, t)$ se definește *morfismul identic* $1_G = (1_V, 1_A)$. Un *izomorfism* de grafuri $h : G \to G'$ este un morfism pentru care există un morfism $k : G' \to G$ astfel încît $h \circ k = 1_{G'}$, $k \circ h = 1_G$; în acest caz, aplicațiile h_A, h_V sînt în mod necesar bijective.

Drumuri într-un graf; arbori

Fixăm un graf orientat $G = (V, A, i, t)$ și un întreg $n \geqslant 1$.

DEFINIȚIA 3.2. Se numește *drum de lungime n în graful G* orice triplet

$$(u, v, d) \in V \times V \times A^*,$$

unde u și v sînt vîrfuri iar $d = a_1 \ldots a_n$ este un cuvînt din dicționarul A^* (adică un șir de arce în G), astfel încît să existe și să fie unice vîrfuri $v_0, v_1, \ldots, v_n$ pentru care

$$u = v_0,\ v = v_n \text{ și } \forall\, k,\ 1 \leqslant k \leqslant n,\ i(a_k) = v_{k-1},$$

$$t(a_k) = v_k \text{ (fig. 3.4).}$$

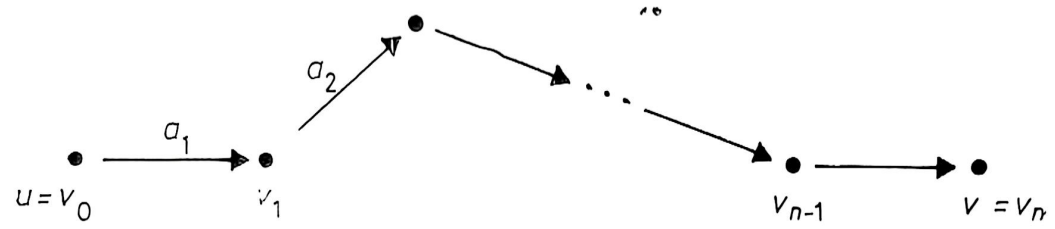


Fig. 3.4

Se mai spune că drumul (u, v, d) *unește* vîrfurile u și v.

Un drum (u, v, d) se numește *închis* dacă $u = v$.

Definiția anterioară se extinde și la cazul $n = 0$, $d = \wedge$ (cuvîntul vid în alfabetul A); în acest caz, $u = v$, iar drumul $(u, \wedge, u)$ se numește drum *nul* în u.

Un graf orientat G se numește *arbore* dacă există un vîrf marcat v_0 (numit *rădăcina* arborelui), cu proprietatea că pentru orice vîrf v din G există și este unic un drum unind v_0 cu v.

Se observă imediat că a defini un drum în graful G de lungime n revine la a da un morfism de grafuri $P_n \to G$, iar un morfism de grafuri $Q_n \to G$ definește un drum închis.

Vom nota cu $d(G)$ mulțimea tuturor drumurilor în graful G.

LEMĂ. *Dacă* $|A| < n$, *atunci pentru orice drum din* $d(G)$ *de lungime n există un arc prin care drumul trece de două ori.*

Demonstrație. Fie $(u, v, d) \in d(G)$ un drum de lungime n trecînd prin vîrfurile $v_0, \ldots, v_n$. Aplicația

$$\varphi : S_n \to A, \quad k \mapsto \text{arcul } (v_k, v_{k+1})$$

nu este injectivă (căci altfel ar rezulta $n \leqslant |A|$), deci există $p, q \in S_n$, $p \neq q$, astfel încît $\varphi(p) = \varphi(q)$. Așadar, există un arc $a \in A$, astfel încît $a = (v_p, v_{p+1}) = (v_q, v_{q+1})$, cu $p \neq q$, ceea ce exprimă riguros faptul că drumul trece de două ori prin arcul a. ∎

Grafuri neorientate

Dacă V este o mulțime, vom numi *pereche neordonată* de elemente din V orice mulțime de forma $\{v_1, v_2\}$ cu $v_1, v_2 \in V$ (nu se exclude cazul $v_1 = v_2$) și vom nota cu $V^{(2)}$ mulțimea acestora. A da un *graf neorientat* $\Gamma = (V, M, \partial)$ revine la a da o mulțime V de *vîrfuri*, o mulțime de *muchii* M și o aplicație $\partial : M \to V^{(2)}$.

Dacă $\partial(m) = \{v_1, v_2\}$, atunci se spune că muchia m *unește* vîrfurile v_1 și v_2. Un *lanț* (sau *drum*) de lungime n în Γ este un șir de muchii $m_1, \ldots, m_n$ astfel încît să existe un șir de vîrfuri $v_0, v_1, \ldots, v_n \in V$ așa încît muchia m_k să unească v_{k-1} și v_k pentru orice $1 \leqslant k \leqslant n$. Se mai spune că acest lanț unește vîrfurile v_0 și v_n. Dacă $v_0 = v_n$, lanțul se numește *ciclu*. Fiind dat un graf neorientat $\Gamma = (V, M, \partial)$, pe mulțimea V se poate introduce relația binară R definită prin : $vRv' \leftrightarrow$ există o muchie din M care unește vîrfurile v și v'. Închiderea ei reflexivă și tranzitivă, $R^* = \bigcup_{n \geqslant 0} R^n$ (§ 1.3) este definită prin

$$vR^*v' \leftrightarrow v = v' \text{ sau există un lanț care unește } v \text{ și } v'$$

și este o relație de echivalență (numită *relația de conexiune* pe V). Pentru orice vîrf $v \in V$ al grafului neorientat Γ, clasa de echivalență a lui v se numește *componenta conexă* a lui v. Graful Γ se numește *conex* dacă orice două vîrfuri sînt echivalente. Remarcăm în fine că oricărui graf orientat i se asociază în mod natural un graf neorientat cu aceeași mulțime de vîrfuri.

Grafuri etichetate și organigrame

Fie $G = (V, A, i, t)$ un graf orientat cu proprietatea că oricare ar fi vîrful $v \in V$, mulțimea $\{a \in A \mid i(a) = v\}$ a arcelor care „ies" din v este finită, cu $r(v)$ elemente. Fixînd o ordonare a acestor arce prin numerotarea

$$(v, 1), \ldots, (v, r(v)),$$

se poate considera o aplicație

$$\varphi : V \to V^*, \qquad v \mapsto c_1 c_2 \ldots c_{r(v)},$$

unde c_k este terminalul arcului (v, k), $1 \leqslant k \leqslant r(v)$.

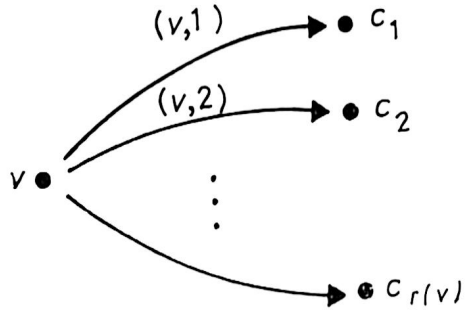


Fig. 3.5

Se spune atunci că G este un *graf etichetat* (*pe arce*).

Un exemplu remarcabil de graf etichetat îl constituie organigramele și, în particular, schemele logice.

Să fixăm o mulțime Σ și o partiție numărabilă a sa,

$$\Sigma = \Sigma_0 \cup \Sigma_1 \cup \Sigma_2 \cup \ldots = \bigcup_{i \in \mathbb{N}} \Sigma_i, \text{ cu } \Sigma_i \cap \Sigma_j = \emptyset \text{ pentru } i \neq j.$$

Fie $z_1, \ldots, z_p$ elemente care nu aparțin lui Σ.

DEFINIȚIA 3.3. Se numește Σ-*organigramă de tip* (n, p) orice triplet $\Omega = (G, j, \varepsilon)$, unde:

1) G este un graf etichetat;

2) $j : S_n \to V$ este o aplicație (numită *funcție de intrare*) care asociază oricărui k, $0 \leqslant k < n$, *intrarea* $j(k) \in V$;

3) o aplicație $\varepsilon : V \to \Sigma \cup \{z_1, \ldots, z_p\}$.

Se presupune în plus că oricărui vîrf $v \in V$, cu $r(v) \geqslant 1$, i se asociază un element din $\Sigma_{r(v)}$, și oricărui vîrf $v \in V$, cu $r(v) = 0$, i se asociază un element din $\Sigma_0 \cup \{z_1, \ldots, z_p\}$; în acest ultim caz, dacă $\varepsilon(v) \in \{z_1, \ldots, z_p\}$, se spune că vîrful v este un *terminal* (*ieșire* sau, cum se mai spune, *frunză*).

Dacă numărul terminalelor este p, dacă ε realizează o corespondență bijectivă între terminale și elementele $z_1, \ldots, z_p$, iar aplicația j este injectivă, atunci se spune că Σ-organigrama Ω de tip (n, p) *are* n *intrări și* p *ieșiri*.

În ipoteza că $\Sigma_0 = \emptyset$, $\Sigma_3 = \Sigma_4 = \ldots = \emptyset$, Σ_1 este mulțimea simbolurilor (etichetelor) de operații iar Σ_2 este mulțimea simbolurilor de predicate, Σ-organigramele se numesc *scheme logice*.

Fie $\Omega' = (G', j', \varepsilon')$ o altă Σ-organigramă de tip (n, p). Prin *morfism de* Σ-*organigrame*

$$h : \Omega \to \Omega'$$

se înțelege un morfism de grafuri $h = (h_V, h_A)$ care păstrează intrările (în sensul că $h_V \circ j = j'$) și, în plus, păstrează ordinea [în sensul că $h_A(v, i) = (h_V(v), i)$ pentru orice arc (v, i), $1 \leqslant i \leqslant r(v)$]. Se definesc în mod natural *compunerea* a două morfisme de Σ-organigrame și *morfismele identice*.

Observații. Rețelele de transport, automatele, organigramele pentru programare etc. sînt tipuri de modele ale unor sisteme distincte care pot fi descrise matematic în termeni de grafuri etichetate, anume de grafuri orientate ale căror arce poartă etichete cu semnificații diferite în cele trei cazuri — costuri de transport, simboluri ale unui alfabet și respectiv transformări de stare reprezentînd semantica matematică a „execuției" arcelor respective. Desigur, sistemele de mai sus au o evoluție dinamică în timp și nu ne putem restrînge la modelarea cu caracter static. În cazul rețelelor de transport ne interesează existența unei rute (drum) între două vîrfuri date. Ne interesează de asemenea o parcurgere fictivă a acestei rute pentru a calcula costul transportului de-a lungul ei adiționînd costurilor ce etichetează arcele componente. În cazul automatelor ne interesează evoluția automatului între două stări de îndată ce s-a primit la intrare un șir de simboluri. Aceasta se obține prin concatenarea simbolurilor care etichetează arcele care compun evoluția automatului. În cazul modelelor de programe, execuția, reprezentată de trecerea fluxului controlului de la un punct la altul al organigramei, se caracterizează prin efectul cumulat (compoziția) transformărilor de stare ce etichetează arcele parcurse.

Încercînd o sinteză a trăsăturilor comune de tip dinamic ale modelelor anterioare, observăm că fiecărui drum în graful respectiv i se atașează o anumită valoare (o *etichetă*) pornind de la etichetele arcelor componente ale drumului. Mulțimea drumurilor grafului admite o structurare algebrică dată de operația de concatenare, iar extinderea etichetării de la arce la drumuri se face în compatibilitate cu această structură. Anume, eticheta unui drum care se obține prin concatenarea altor două drumuri se poate recupera din etichetele acestora din urmă printr-o operație sistematic aceeași. Deoarece arcele individuale sînt și ele cazuri particulare de drumuri, se impune firesc ideea de a include în model și o anumită structură algebrică ce trebuie să caracterizeze mulțimea etichetelor (de arce sau de drumuri). Concatenarea drumurilor este asociativă. Este util (de exemplu, din motive de uniformitate a expunerii) să fie considerate și drumuri de lungime nulă, care încep și se termină în același vîrf și fără a conține vreun arc. Iată că în mod natural structura algebrică a mulțimii etichetelor trebuie să fie *una de monoid*. În cazul rețelelor de transport acesta este monoidul $(\mathbb{R}_+, +, \circ)$ al numerelor reale $\geqslant 0$. În cazul automatelor se consideră dicționarul unui anumit alfabet, iar în cazul organigramelor se consideră monoidul Rel S al relațiilor binare pe mulțimea S a stărilor programului. Așadar, este pe deplin justificat studiul algebric al unor asociații între un graf, un monoid și o aplicație de etichetare asociind fiecărui arc al grafului un element din monoid. În acest context apare în mod firesc utilitatea conceptului de categorie.

Noțiunea de categorie

Ideea principală în elaborarea noțiunii de categorie constă în studiul sistematic al claselor de obiecte și al unor legături structurale între obiecte; în analogie cu axiomatica Zermelo-Fraenkel a teoriei mulțimilor se poate dezvolta o axiomatică în care se ia ca noțiune primară *clasa* (și nu mulțimea), presupunînd că între clase există relația de apartenență $\in$. Mulțimile și elementele sînt cazuri particulare de clase. Dacă A, B sînt clase și $A \in B$, se spune că A este un *element* al lui B, iar dacă $\forall X, X \in A \Rightarrow X \in B$, se spune că A este *inclusă* în B și se scrie $A \subset B$. Dacă $A \subset B$ și $B \subset A$, atunci clasele A și B se numesc *egale*. În acest context, se numește *mulțime* orice clasă care este un element al unei clase; se notează cu **Set** clasa tuturor mulțimilor (**Set** nu este mulțime!).

DEFINIȚIA 3.4. *O categorie*

$$\mathbf{C} = (V, A, i, t, \circ, 1)$$

este un 6-uplu constînd din:

1) o clasă V de *obiecte* și o clasă A de *morfisme*;

2) două aplicații $i, t : A \to V$;

3) o operație de *compunere* $A \times A \to A$, $(a, a') \mapsto a' \circ a$ definită pe perechile de morfisme (a, a'), astfel încît $t(a) = i(a')$; în plus, se presupune că

$$i(a' \circ a) = i(a), \qquad t(a' \circ a) = t(a'),$$

iar compunerea este asociativă: $a'' \circ (a' \circ a) = (a'' \circ a') \circ a$, în cazul cînd cei doi membri au sens.

4) o funcție $1 : V \to A$ care asociază oricărui obiect $v \in V$ un morfism $1_v \in A$ (notat $v \xrightarrow{1_v} v$), numit *morfismul identic* al lui v și satisfăcînd relațiile

$$1_{t(a)} \circ a = a \text{ și } a \circ 1_{i(a)} = a,$$

pentru orice morfism $a \in A$.

În cazul cînd clasele V și A sînt mulțimi, categoria $\mathbf{C}$ se numește *categorie mică*.

Remarcăm o analogie foarte strînsă între noțiunile de categorie și de graf orientat. Vîrfurile se numesc acum obiecte, iar arcele — morfisme. Într-o categorie este considerată operația de compunere a morfismelor (care nu este peste tot definită!) și pentru fiecare obiect este fixat cîte un morfism marcat care acționează ca un element neutru relativ la compunere. Ca și în cazul grafurilor orientate, scriem $a : v \to v'$ (sau $v \xrightarrow{a} v'$) atunci cînd $v = i(a)$, $v' = t(a)$. Vom nota

$$\mathbf{C}(v, v') = \{a \in A \mid v \xrightarrow{a} v'\}.$$

Dacă $a \in \mathbf{C}(v, v')$ și $a' \in \mathbf{C}(v', v'')$, atunci are sens $a' \circ a$; compunerea este o funcție totală

$$\mathbf{C}(v, v') \times \mathbf{C}(v', v'') \to \mathbf{C}(v, v''), \ (a, a') \mapsto a' \circ a.$$

Trebuie de asemenea remarcat că în cazul grafurilor V și A erau mulțimi, în timp ce în cazul categoriilor ele pot fi și clase.

Facem convenția ca pentru o categorie $\mathbf{C}$ să notăm cu $\mathrm{Ob}\,\mathbf{C}$ clasa obiectelor sale și cu $\mathrm{Mor}\,\mathbf{C}$ clasa morfismelor lui $\mathbf{C}$. În categorii distincte simbolurile inițialului, terminalului, compunerii, morfismului identic vor fi notați i, t, $\circ$, 1, respectiv, ceea ce simplifică notația și nu introduce ambiguități necontrolabile.

Un morfism $u : A \to B$ într-o categorie $\mathbf{C}$ se numește *izomorfism* dacă există un morfism $v : B \to A$ (numit *inversul* lui u), astfel încît $v \circ u = 1_A$ și $u \circ v = 1_B$.

Subcategorii

Dacă $\mathbf{C}$ și $\mathbf{C}'$ sînt două categorii, se spune că $\mathbf{C}'$ este o *subcategorie* a lui $\mathbf{C}$ și se scrie $\mathbf{C}' \hookrightarrow \mathbf{C}$, dacă $\mathrm{Ob}\,\mathbf{C}' \subset \mathrm{Ob}\,\mathbf{C}$, $\mathrm{Mor}\,\mathbf{C}' \subset \mathrm{Mor}\,\mathbf{C}$ și, în plus, toate operațiile din $\mathbf{C}'$ sînt restricțiile operațiilor corespunzătoare din $\mathbf{C}$.

Să presupunem că avem $\mathbf{C}' \subset \mathbf{C}$. Dacă $\mathrm{Ob}\,\mathbf{C}' \subset \mathrm{Ob}\,\mathbf{C}$, se spune că $\mathbf{C}'$ este o subcategorie *stricta* a lui $\mathbf{C}$, iar dacă pentru orice obiecte $v_1, v_2 \in \mathrm{Ob}\,\mathbf{C}$ avem $\mathbf{C}(v_1, v_2) = \mathbf{C}'(v_1, v_2)$, atunci se spune că $\mathbf{C}'$ este o subcategorie *plină* a lui $\mathbf{C}$.

Exemple de categorii

1) Notăm cu **Set** categoria mulțimilor; obiectele ei sînt toate mulțimile iar morfismele — funcții totale între mulțimi; compunerea de morfisme este cea uzuală, iar morfismul identic al unui obiect A este aplicația identică 1_A.

Dacă S este o mulțime fixată de indici, atunci se poate considera categoria $\mathbf{Set}_S$ în care toate obiectele sînt familiile de mulțimi $\mathcal{A} = \{A_s\}_{s \in S}$ indexate după S, iar morfismele — familii de aplicații $f : \mathcal{A} \to \mathcal{B}$, $f = \{f_s\}_{s \in S}$, $f_s : A_s \to B_s$, compunerea făcîndu-se pe componente.

Se poate de asemenea considera categoria **Rel** a relațiilor, în care obiectele sînt mulțimi iar morfismele — relațiile binare între mulțimi, compunerea fiind compunerea de relații definită în § 1.1, iar morfismul identic al unui obiect A este relația 1_A. **Set** este o subcategorie strictă a lui **Rel**.

2) Se pot defini categoria **Mon** a monoizilor (obiectele fiind monoizii, morfismele — morfismele de monoizi și compunerea — uzuală), categoria **Gr** a grupurilor, categoria semimodulelor peste un 1/2-inel fixat, toate fiind subcategorii ale lui **Set**.

Dacă X este o mulțime, se poate considera categoria X-**Din** a X-dinamicilor (obiectele fiind X-dinamicile iar morfismele — morfismele de X-dinamici definite în § 1.4, compunerea — uzuală).

3) Fie **Nat** categoria în care obiectele sînt numere naturale, $\mathrm{Ob}\,(\mathbf{Nat}) = \mathbb{N}$ și pentru orice două obiecte m, n, $\mathrm{Mor}\,(m, n)$ este mulțimea tuturor funcțiilor $S_m \to S_n$. Mai general, dacă A este o mulțime oarecare, se poate considera categoria $\mathbf{C} = A^-$**cuv** în care obiectele sînt cuvinte peste alfabetul A (adică $\mathrm{Ob}\,\mathbf{C} = A^*$) și pentru orice două cuvinte w, w',

$$\mathbf{C}(w, w') = \begin{array}{l}\{\text{funcțiile } f : S_{l(w)} \to S_{l(w')} \text{ astfel încît pentru literele corespunzătoare}\\ \text{avem } w_i = w'_{f(i)} \text{ oricare ar fi } 0 \leqslant i < l(w)\}.\end{array}$$

Aceste două categorii joacă un rol important în studiul algebrei multisortate.

4) Fie $(M, *, e)$ un monoid. Atunci se poate considera categoria $\mathbf{C}$ avînd un singur obiect, anume M și ca morfisme elementele lui M. Așadar, $\mathrm{Ob}\,\mathbf{C} = \{M\}$ și $\mathrm{Mor}\,\mathbf{C} = M$. Pentru orice morfisme $a, b \in M$ compunerea este $a * b$ și $1_M = e$. Invers, orice categorie avînd un singur obiect definește un monoid.

Fie $(P, \leqslant)$ o mulțime ordonată. Atunci se poate considera categoria mică $\mathbf{C}$ în care obiectele sînt elementele lui P, $\mathrm{Ob}\,\mathbf{C} = P$ și $\mathrm{Mor}\,\mathbf{C}$ este mulțimea perechilor de obiecte $(u, v) \in P \times P$ astfel încît $u \leqslant v$. Compunerea: $(v, w) \circ (u, v) = (u, w)$ folosind tranzitivitatea relației de ordine $\leqslant$, iar $1_u = (u, u)$ folosind reflexivitatea. Invers, pentru orice categorie mică $\mathbf{C}$ se poate defini o relație de preordine pe $\mathrm{Ob}\,\mathbf{C}$, punînd $u \leqslant v \leftrightarrow \mathbf{C}(u, v) \neq \emptyset$.

5) Un exemplu de categorie îl constituie categoria **Graf** a grafurilor orientate, morfismele — morfisme de grafuri, iar compunerea de morfisme este cea descrisă (p. 111).

6) Dăm acum un exemplu remarcabil de categorie, care va fi folosit ulterior în teoria automatelor și, în particular, în obținerea unei extinderi a teoremei lui Kleene (teorema 4.9).

Fie $G = (V, A, i, t)$ un graf orientat fixat. Notăm cu $A^\# = d(G)$, mulțimea tuturor drumurilor în G (incluzînd pentru fiecare vîrf $v \in V$ cîte un drum vid $(v, v, \wedge)$, care începe și se termină în vîrful v). Definim apoi aplicațiile $i^\#, t^\# : A^\# \to V$ care asociază fiecărui drum (u, v, d) inițialul u și, respectiv, terminalul v al drumului. Se obține astfel un nou graf $G^\# = (V, A^\#, i^\#, t^\#)$ care extinde G, în sensul că există o aplicație injectivă $A \to A^\#$ și $i^\# | A = i$, $t^\# | A = t$. În graful $G^\#$ se poate evidenția o structură algebrică specifică. Să considerăm mulțimea perechilor de drumuri concatenabile, anume

$$A^\bullet \times_V A^\# = \{(\delta_1, \delta_2) \in A^\# \times A^\# \mid t^\#(\delta_1) = i^\#(\delta_2)\}.$$

Atunci se poate defini concatenarea $c : A^\# \times_V A^\# \to A^\#$, care apare ca o operație algebrică (binară) nu peste tot definită pe $A^\#$. Evident, $\forall (\delta_1, \delta_2) \in A^\# \times_V A^\#$ avem

$$i^\#(c(\delta_1, \delta_2)) = i^\#(\delta_1) \quad \text{și} \quad t^\#(c(\delta_1, \delta_2)) = t^\#(\delta_2).$$

Împreună cu aplicația $1 : V \to A^\#$, care asociază fiecărui vîrf $v \in V$ drumul vid $(v, v, \wedge)$, aplicația c are următoarele proprietăți :

i) asociativitatea : $\forall (\delta_1, \delta_2) \in A^\# \times_V A^\#$, $(\delta_2, \delta_3) \in A^\# \times_V A^\#$ avem $(c(\delta_1, \delta_2), \delta_3) \in A^\# \times_V A^\#$, $(\delta_1, c(\delta_2, \delta_3)) \in A^\# \times_V A^\#$ și $c(c(\delta_1, \delta_2), \delta_3) = c(\delta_1, c(\delta_2, \delta_3))$;

ii) existența elementelor neutre : $\forall v \in V$ și $\forall \delta \in A^\#$, $i^\#(\delta) = v$ avem $c(1(v), \delta) = \delta$; $\forall v \in V$ și $\forall \delta \in A^\#$, $t^\#(\delta) = v$ avem $c(\delta, 1(v)) = \delta$.

În concluzie, 6-uplul $(V, A^\#, i^\#, t^\#, c, 1)$ constituie o categorie, numită *categoria drumurilor în graful* G și notată $\mathbf{d}(G)$. Pe scurt, obiectele acestei categorii sînt vîrfurile lui G și morfismele sînt drumurile în G, $\mathrm{Ob}\,\mathbf{d}(G) = V$ și $\mathrm{Mor}\,\mathbf{d}(G) = A^\#$. Pentru orice drumuri $(u, v, d), (v, w, d')$, concatenarea (compunerea) lor este drumul $(u, w, j(d, d'))$ care este un drum de la u la w, iar cuvintele d, d' se concatenează în A^*. Morfismul identic al unui vîrf $v \in V$ este drumul $1(v) = (v, v, \wedge)$.

7) Am definit anterior (definiția 3.3) conceptul de Σ-organigramă și morfismele între Σ-organigrame. Se poate atunci considera categoria $\Omega_\Sigma(n, p)$ a Σ-organigramelor de tip (n, p). O Σ-organigramă de tip (n, p) se numește *accesibilă* dacă $\forall v \in V$, $\exists k \in S_n$ astfel încît $\mathbf{d}_G(j(k), v) \neq 0$. Ca un fapt remarcabil, se poate demonstra că pentru orice două Σ-organigrame accesibile Ω, Ω' există cel mult un morfism $\Omega \to \Omega'$.

Obiecte inițiale, obiecte terminale

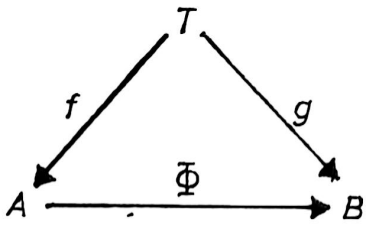
DEFINIȚIA 3.5. Fie $\mathbf{C}$ o categorie. Un obiect $I \in \mathrm{Ob}\,\mathbf{C}$ (resp. $T \in \mathrm{Ob}\,\mathbf{C}$) se numește obiect *inițial* (resp. obiect *terminal*) în $\mathbf{C}$ dacă pentru orice $A \in \mathrm{Ob}\,\mathbf{C}$ există și este unic un morfism $I \to A$ (resp. $A \to T$).

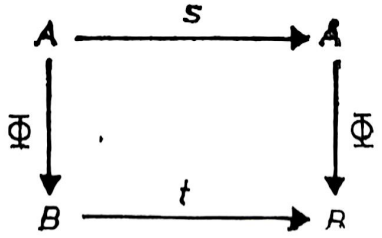
Dacă există, obiectele inițiale (resp. terminale) sînt evident unice pînă la un izomorfism.

Exemple. 1) În categoria **Set** mulțimea vidă este obiect inițial iar $\mathbf{1}$ este obiect terminal.

2) Un graf orientat G este un arbore cu rădăcina v_0 dacă și numai dacă v_0 este un obiect inițial în categoria $\mathbf{d}(G)$.

3) Fie $\mathbf{C}$ o categorie avînd un obiect terminal T. Se spune că un obiect $A \in \mathrm{Ob}\,\mathbf{C}$ *are structură Peano în* $\mathbf{C}$ dacă există o pereche de morfisme $f : T \to A$, $s : A \to A$ în $\mathbf{C}$, astfel încît $\forall B \in \mathrm{Ob}\,\mathbf{C}$, $\forall g : T \to B$, $t : B \to B$ (din $\mathrm{Mor}\,\mathbf{C}$) să existe și să fie unic un morfism $\Phi : A \to B$ făcînd comutative diagramele





Este evident că orice două obiecte avînd structură Peano sînt izomorfe.

În cazul cînd $\mathbf{C} = \mathbf{Set}$ și $T = \mathbf{1} = \{\wedge\}$, mulțimea $\mathbb{N}$ are structură Peano în **Set**. Într-adevăr, să considerăm aplicația nulă $f : T \to \mathbb{N}$, $\wedge \mapsto 0$ și funcția succesor $s : \mathbb{N} \to \mathbb{N}$. Pentru orice mulțime B și pentru orice aplicații $g : T \to B$, $\wedge \mapsto b$; $t : B \to B$, este defi-

rută o dinamică cu inițializare $(B, l)_b$; conform teoremei 1.1, există și este unic un morfism de dinamici $(\mathbb{N}, s) \xrightarrow{\Phi} (B, l)$, deci o aplicație $\Phi : \mathbb{N} \to B$ astfel încît $\Phi(0) = b$ și $\Phi \circ s = l \circ \Phi$, ceea ce trebuia demonstrat.

Remarcăm în fine că dinamicile cu inițializare și morfismele corespunzătoare formează o categorie în care $(\mathbb{N}, s)_0$ este un obiect inițial ([10]).

Functori

Am definit anterior conceptul de categorie. Ca de obicei, se impune formularea unei definiții corespunzătoare pentru un concept de morfism între două categorii, care poartă numele specific de functor.

DEFINIȚIA 3.6. Se numește *functor*

$$\mathbf{F} : \mathbf{C} \to \mathbf{C}'$$

între două categorii $\mathbf{C}$, $\mathbf{C}'$ o pereche de funcții

$$\mathbf{F}_V : \mathrm{Ob}\,\mathbf{C} \to \mathrm{q}\mathbf{C}', \qquad \mathbf{F}_A : \mathrm{Mor}\,\mathbf{C} \to \mathrm{Mor}\,\mathbf{C}'$$

care conservă inițialele, terminalele, compunerile și morfismele identice, adică

$$i \circ \mathbf{F}_A = \mathbf{F}_V \circ i,\ t \circ \mathbf{F}_A = \mathbf{F}_V \circ t \quad \text{și} \quad \forall\, u, u', v,\ \mathbf{F}_A(u' \circ u) =$$

$$= \mathbf{F}_A(u') \circ \mathbf{F}_A(u) \quad \text{și} \quad \mathbf{F}_A(1_v) = 1_{\mathbf{F}_V}(v).$$

Fiind dați doi functori $\mathbf{F} : \mathbf{C} \to \mathbf{C}'$, $\mathbf{G} : \mathbf{C}' \to \mathbf{C}''$, se definește *compusul* lor $\mathbf{G} \circ \mathbf{F} : \mathbf{C} \to \mathbf{C}''$ (notat uneori $\mathbf{FG}$), ca fiind functorul $\mathbf{H}$ pentru care pe obiecte $\mathbf{H}(v) = \mathbf{G}(\mathbf{F}(v))$, $\forall\, v \in \mathrm{Ob}\,\mathbf{C}$ și pe morfisme, $\mathbf{H}(f) = \mathbf{G}(\mathbf{F}(f))$, $\forall\, f \in \mathrm{Mor}\,\mathbf{C}$. Se verifică ușor că $\mathbf{H}$ este într-adevăr un functor, iar compunerea de functori este asociativă. În plus, pentru orice categorie $\mathbf{D}$ există *functorul identic* $1_{\mathbf{D}} : \mathbf{D} \to \mathbf{D}$, definit prin

$$1_{\mathbf{D}}(v) = v,\ \forall\, v \in \mathrm{Ob}\,\mathbf{D} \text{ și } 1_{\mathbf{D}}(f) = f,\ \forall\, f \in \mathrm{Mor}\,\mathbf{D}.$$

Functorul identic este elementul neutru pentru compunerea de functori în sensul că $\mathbf{F} \circ 1_{\mathbf{D}} = \mathbf{F}$ și $1_{\mathbf{D}} \circ \mathbf{F} = \mathbf{F}$ etc.

În acest mod este definită o nouă entitate matematică — categoria categoriilor, notată **Cat**, în care obiectele sînt categorii, iar morfismele — functorii. Categoriile mici formează o subcategorie $\mathbf{Cat}_m \hookrightarrow \mathbf{Cat}$.

Exemple. 1) Considerăm categoriile $\mathbf{C} = \mathbf{Graf}$ și $\mathbf{C}' = \mathbf{Set}$. Un exemplu de functor $\mathbf{U} : \mathbf{C} \to \mathbf{C}'$ se obține astfel : oricărui graf $G = (V, A, i, t)$ i se asociază mulțimea vîrfurilor, $\mathbf{U}(G) = V$ și oricărui morfism $h : G \to G'$, $h = (h_V, h_A)$ de grafuri i se asociază aplicația de mulțimi $\mathbf{U}(h) = h_V : V \to V'$. Acest functor se numește uneori *șterg ător*, pentru că prin aplicarea lui se omite o parte din structura oricărui graf.

Adeseori în definirea functorilor ne restrîngem la a indica doar corespondența pe obiecte.

2) Un alt functor ștergător este $\mathbf{U} : \mathbf{Mon} \to \mathbf{Set}$, obținut asociind oricărui monoid mulțimea sa suport și oricărui morfism de monoizi aplicația corespunzătoare de mulțimi. Se poate de asemenea considera functorul $\mathbf{G} : \mathbf{Set} \to \mathbf{Mon}$ care asociază oricărei mulțimi A monoidul $A^* = \mathbf{G}(A)$ liber generat de A și oricărei aplicații de mulțimi $f : A \to B$, morfismul de monoizi $\mathbf{G}(f)$ $f^* : A^* \to B^*$ construit în corolarul teoremei 1.7. Proprietatea de universalitate exprimată în teorema 1.7 arată că pentru orice mulțime A și pentru orice monoid B, aplicația de mulțimi

$$\mathrm{Mon}(\mathbf{G}(A), B) \to \mathrm{Set}(A, \mathbf{U}(B)), \qquad F \mapsto F \circ I_A$$

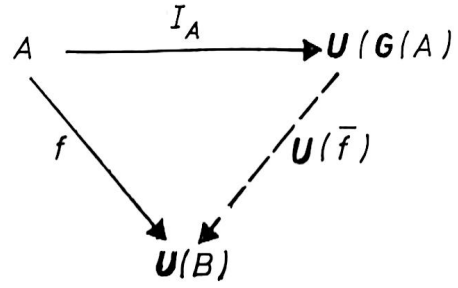
este bijectivă.

Obiecte liber generate

Situația din exemplul 2) anterior sugerează definiția următoare.

DEFINIȚIA 3.7. Fie $\mathbf{U} : \mathbf{C} \to \mathbf{C}'$ un functor, $\mathbf{G} : \mathrm{Ob}\,\mathbf{C}' \to \mathrm{Ob}\,\mathbf{C}$ o aplicație și $\{I_A\}_{A \in \mathrm{Ob}\,\mathbf{C}'}$ o familie de morfisme $I_A : A \to \mathbf{U}(\mathbf{G}(A))$, indexată după obiectele lui $\mathbf{C}'$. Se spune că $\mathbf{U}$ *are adjunct*, iar $\mathbf{G}(A)$ este un $\mathbf{C}$-*obiect liber generat de* A dacă este îndeplinită următoarea condiție :

(*) pentru orice $B \in \mathrm{Ob}\,\mathbf{C}$ și pentru orice morfism $f : A \to \mathbf{U}(B)$ în categoria $\mathbf{C}'$, există și este unic un morfism $\bar{f} : \mathbf{G}(A) \to B$ în $\mathbf{C}$, astfel încît $\mathbf{U}(\bar{f}) \circ I_A = f$, adică este comutativă diagrama



În acest caz este bine determinat un functor $\mathbf{G} : \mathbf{C}' \to \mathbf{C}$ (numit *adjunctul lui* $\mathbf{U}$); anume, pentru orice morfism $a : A \to A'$ în $\mathbf{C}'$ se consideră morfismul $f = I_{A'} \circ a : A \to \mathbf{U}(\mathbf{G}(A'))$ și $\mathbf{G}(a) : \mathbf{G}(A) \to \mathbf{G}(A')$ este acel unic morfism pentru care $\mathbf{U}(\mathbf{G}(a)) \circ I_A = I_{A'} \circ a$. Se arată ușor că orice doi adjuncți ai lui $\mathbf{U}$ sînt izomorfi.

Un rezultat important îl constituie următorul.

TEOREMA 3.1. *Functorul ștergător* $\mathbf{U} : \mathbf{Cat}_m \to \mathbf{Graf}$, *care asociază oricărei categorii mici* $\mathbf{C} = (V, A, i, t, \circ, 1)$ *graful* (V, A, i, t) *are*

adjunct, anume functorul $\mathbf{d} : \mathbf{Graf} \to \mathbf{Cat}_m$, *care asociază oricărui graf* G *categoria* $\mathbf{d}(G)$ *a drumurilor în acel graf.*

(Aşadar, $\mathbf{d}(G)$ este obiectul liber generat de G.)

Demonstraţie. Verificăm condiţiile din definiţia 3.7 şi pentru aceasta considerăm aplicaţia

$$\mathbf{d} : \mathrm{Ob}(\mathbf{Graf}) \to \mathrm{Ob}(\mathbf{Cat}_m),\ G \mapsto \mathbf{d}(G),$$

asociind oricărui graf G categoria drumurilor în G. De asemenea, pentru orice graf G considerăm morfismul de grafuri

$$I_G : G \to \mathbf{U}(\mathbf{d}(G)),$$

care conservă vîrfurile şi asociază oricărui arc a din G drumul $(i(a), t(a), a)$.

Avem de arătat că pentru orice categorie mică $\mathbf{C}$ şi pentru orice morfism de grafuri $f : G \to \mathbf{U}(\mathbf{C})$, există şi este unic un functor $\overline{\mathbf{f}} : \mathbf{d}(G) \to \mathbf{C}$, astfel încît $\mathbf{U}(\overline{\mathbf{f}}) \circ I_G = f$. Este suficient să asociem oricărui vîrf $v \in V$, obiectul $f(v)$ din $\mathbf{C}$ şi oricărui drum în G, $d = (u, v, a_1 \ldots a_n)$ obiectul $\overline{\mathbf{f}}(d) = f(a_1) \circ \ldots \circ f(a_n)$. Verificările necesare sînt imediate. ∎

§ 3.2. ELEMENTE DE ALGEBRĂ UNIVERSALĂ

Înainte de a adînci studiul arborilor şi aplicaţiile lor la sisteme dinamice discrete, este necesar să introducem cîteva noţiuni de algebră universală, care se referă la studiul general al operaţiilor algebrice şi al implementării acestora pe mijloace mecanizate.

Signatură

Reamintim că dacă M este o mulţime, prin operaţie n-ară ($n \in \mathbb{N}$) pe M se înţelege orice aplicaţie $\omega : M^n \to M$. Se mai spune că operaţia ω are ordinul de aritate n. Aşadar, oricărui sistem ordonat $(x_1, \ldots, x_n)$ de elemente din M i se asociază un element bine determinat, notat $\omega(x_1, \ldots, x_n)$ sau $x_1 \ldots x_n\omega$. O operaţie nulară (0-ară) revine la fixarea unui element din M. Mulţimea tuturor operaţiilor posibile pe mulţimea M este

$$\mathrm{Op}\ M = \bigcup_{n \geqslant 0} (M)^{M^n} \qquad \text{(reuniune disjunctă).}$$

Se poate considera funcţia de aritate

$$\nu_M : \mathrm{Op}\ M \to \mathbb{N},$$

care asociază fiecărei operații $\omega \in \mathrm{Op}\, M$, ordinul ei de aritate. Mulțimea operațiilor n-are pe M este $\{\omega \in \mathrm{Op}\, M \mid \nu_M(\omega) = n\}$.

DEFINIȚIA 3.8. Se numește *signatură* orice pereche (Ω, ν) alcătuită dintr-o mulțime Ω și o aplicație $\nu : \Omega \to \mathbb{N}$. Elementele lui Ω se mai numesc *simboluri* de operații (sau *etichete*).

Pentru orice $n \in \mathbb{N}$ se notează $\Omega_n = \{\omega \in \Omega \mid \nu(\omega) = n\}$. Așadar, $\Omega = \bigcup_{n \in \mathbb{N}} \Omega_n$ (reuniune disjunctă).

Exemple. 1) Fie $\Omega = \{+, \circ, \mathrm{T}\}$ cu $\nu(+) = \nu(\circ) = 2$ și $\nu(\mathrm{T}) = 0$. Se obține o signatură cu două simboluri de operații binare și un simbol de operație nulară.

2) Dacă M este o mulțime, putem lua $\Omega = \mathrm{Op}\, M$, mulțimea operațiilor pe M și $\nu = \nu_M$ funcția de aritate.

3) Dacă V este un spațiu vectorial real, atunci se poate considera signatura

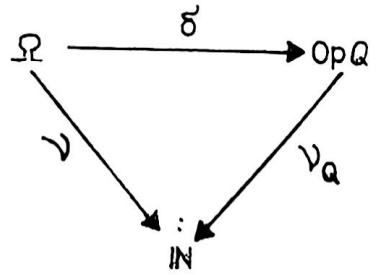
$$\Omega = \{+\} \cup \{\omega_\lambda\}_{\lambda \in \mathbb{R}},$$

unde $+$ este eticheta adunării în V, iar $\omega_\lambda : V \to V$, $x \mapsto \lambda x$ operația de înmulțire cu scalarul λ (identificată cu eticheta ei); aritățile respective sînt $\nu(+) = 2$ și $\nu(\omega_\lambda) = 1$ pentru orice $\lambda \in \mathbb{R}$.

Algebre peste o signatură dată

Putem da acum definiția unui concept fundamental.

DEFINIȚIA 3.9. Fie (Ω, ν) o signatură. Se numește Ω-*algebră* (sau *algebră universală de signatură* Ω) orice pereche (Q, δ) formată dintr-o mulțime Q, numită *mulțimea de bază* (sau *suportul*) Ω-algebrei și o aplicație $\delta : \Omega \to \mathrm{Op}\, Q$, astfel încît $\forall\, \omega \in \Omega$ aritatea operației $\delta(\omega)$ să fie egală cu $\nu(\omega)$, adică să fie comutativă diagrama

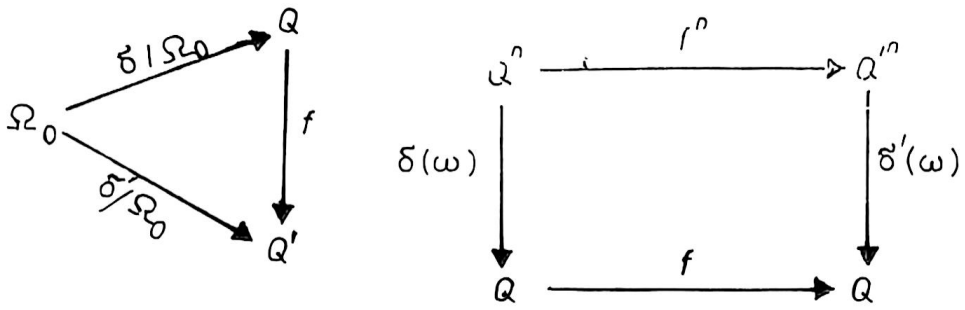


Fie (Q, δ) și (Q', δ') două Ω-algebre. Se numește *morfism de la* (Q, δ) *la* (Q', δ') orice aplicație de mulțimi $f : Q \to Q'$ astfel încît pentru orice $\omega \in \Omega$ și pentru orice $n = \nu(\omega)$ elemente $a_1, \ldots, a_n \in Q$, să aibă loc relația

$$f(\delta(\omega)(a_1, \ldots, a_n)) = \delta'(\omega)(f(a_1), \ldots, f(a_n)).$$

Pentru $n = 0$ aceasta revine la faptul că $\forall\, \omega \in \Omega$, cu $\nu(\omega) = 0$, avem $f(\delta(\omega)) = \delta'(\omega)$. Notînd pentru orice $n \in \mathbb{N}$, $\Omega_n = \{\omega \in \Omega \mid \nu(\omega) =$

$= n\}$, rezultă atunci că $\forall\, \omega \in \Omega_n$ diagramele următoare sînt comutative:



[am notat $f^n : Q^n \to Q'^n$, $(a_1, \ldots, a_n) \mapsto (f(a_1), \ldots, f(a_n))$].

Se mai spune că un morfism f ca mai sus păstrează operațiile din signatura Ω.

Compunerea a două morfisme de Ω-algebre se definește în mod natural; de asemenea, pentru orice Ω-algebră se poate considera morfismul ei identic. Se verifică fără dificultate că *Ω-algebrele și morfismele de Ω-algebre formează o categorie*, notată **Ω-alg**. Dacă $f : Q \to Q'$ este un morfism de Ω-algebre și f este aplicație bijectivă, atunci $f^{-1} : Q' \to Q$ este de asemenea un morfism; în acest caz se spune că f este un izomorfism, iar Ω-algebrele Q, Q' se numesc izomorfe.

Exemple. 1) Fie $\Omega = \{*, e\}$ cu $\nu(*) = 2$, $\nu(e) = 0$. Un monoid $(Q, *_Q, e_Q)$ este o Ω-algebră, definind

$$\delta : \Omega \to \operatorname{Op} S, \quad \begin{cases} * \mapsto \text{operația binară } *_Q \text{ pe } Q, \\ e \mapsto e_Q = \text{fixarea elementului neutru din } Q. \end{cases}$$

Orice morfism de monoizi este un morfism de Ω-algebre.

2) Inelele pot fi considerate ca Ω-algebre, unde $\Omega = \{0, -, +, \cdot\}$; $\nu(0)=0$, $\nu(-) = 1$, $\nu(+) = 2$, $\nu(\cdot) = 2$; dar astfel de Ω-algebre nu sînt în mod necesar inele.

3) Mulțimile pot fi considerate ca Ω-algebre pentru $\Omega = \emptyset$.

4) Să considerăm o X-dinamică (A, δ), în sensul definiției 1.13; este definită atunci în mod natural o aplicație $\delta : X \to A^A$, $x \mapsto \delta_x$, unde $\delta_x : A \to A$, $a \mapsto \delta(a, x)$. Dacă se consideră signatura $\Omega = \{\delta_x\}_{x \in X}$ având toate simbolurile de operație unare, atunci orice X-dinamică A este o Ω-algebră și morfismele de X-dinamici sînt morfisme de Ω-algebre.

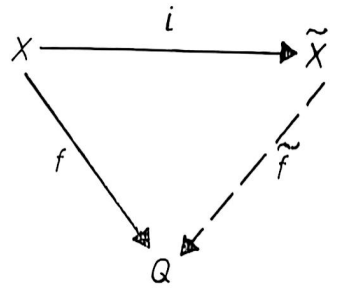
Dăm cîteva definiții importante prin caracterul lor de generalitate și valabile pentru fiecare structură algebrică particulară. Fie (Q, δ), pe scurt Q, o Ω-algebră. O *subalgebră* a lui Q este o submulțime $Q_1 \subset Q$, astfel încît $\forall\, \omega \in \Omega_0$ să avem $\delta(\omega) \in Q_1$ (deci Q_1 conține toate elementele din Q fixate prin operații nulare) și, în plus, $\forall\, n$, $\forall\, \omega \in \Omega_n$, $\forall\, a_1, \ldots, a_n \in Q_1$, să avem $\delta(\omega)(a_1, \ldots, a_n) \in Q_1$; așadar, funcția δ are valori în $\operatorname{Op} Q_1$ și incluziunea $Q_1 \subset Q$ este morfism de Ω-algebre de la (Q_1, δ) la (Q, δ); se mai scrie $Q_1 \hookrightarrow Q$. Dacă (Q, δ) este o Ω-algebră și P este o submulțime a lui Q, atunci intersecția tuturor subalgebrelor lui Q, care conțin P, este o subalgebră a lui Q, cea

mai mică subalgebră care conține P (numită *subalgebra lui Q generată de P* și notată $\langle P\rangle_\Omega$ (sau $\overline{P}$)).

O întrebare firească este următoarea : *fiind dată o signatură Ω, ce mulțimi admit o structură de Ω-algebră ?* Răspunsul nu este imediat ; de exemplu, se poate arăta că pe orice mulțime se poate introduce o structură de grup, dar o mulțime finită are o structură de corp dacă și numai dacă numărul ei de elemente este de forma p^n (cu $p \geqslant 2$ prim și $n \geqslant 1$), așa cum am văzut în § 2.4. Un răspuns este totuși cuprins în următoarea teoremă.

TEOREMA 3.2. *Fie (Ω, ν) o signatură fixată. Pentru orice mulțime X există o Ω-algebră $\widetilde{X}$ și o aplicație de mulțimi $i : X \to \widetilde{X}$, astfel încît să aibă loc următoarea proprietate de universalitate :*

pentru orice Ω-algebră (Q, δ) și pentru orice aplicație de mulțimi $f : X \to Q$, există și este unic un morfism de Ω-algebre $\tilde{f} : \widetilde{X} \to Q$ făcînd comutativă diagrama



Demonstrație. Mulțimea $\widetilde{X}$ va fi construită cu ajutorul mulțimilor X_n, $n \in \mathbb{N}$, definite prin inducție astfel :

1) X_0 este reuniunea disjunctă (suma) mulțimilor X și Ω_0 ;

2) presupunînd $n \in \mathbb{N}$ fixat și X_m definite pentru $0 \leqslant m < n$, definim

$$X_n = \left\{(\omega, a_1, \ldots, a_k) \mid \omega \in \Omega_k,\ a_i \in X_{m_i},\ \sum_{i=1}^{k} m_i = n - 1\right\} ;$$

3) se pune $\widetilde{X} = \bigcup_{n \in \mathbb{N}} X_n$.

Înzestrăm acum mulțimea $\widetilde{X}$ ca Ω-algebră. Anume, pentru orice $\omega \in \Omega$

4) dacă $\omega \in \Omega_k$, $a_1, \ldots, a_k \in \widetilde{X}$, atunci punem $\omega(a_1, \ldots, a_k) = (\omega, a_1, \ldots, a_k)$; în particular, dacă $\omega \in \Omega_0$, atunci $\omega_{\widetilde{X}}$ este elementul ω al lui X_0.

Se verifică imediat că $\widetilde{X}$ este o Ω-algebră.

Definim apoi aplicația

$$i : X \to \widetilde{X}, \quad x \mapsto x \in X_0.$$

Vom demonstra acum proprietatea de universalitate. Fie Q o Ω-algebră oarecare și $f: X \to Q$ o aplicație. Trebuie să arătăm că există și este unic un morfism de Ω-algebre $\tilde{f}: \tilde{X} \to Q$ astfel încît $\tilde{f} \circ i = f$. Pentru aceasta vom construi inductiv restricțiile $f_n = \tilde{f}|X_n$, $\forall\, n \in \mathbb{N}$ și vom arăta că fiecare f_n este bine determinată de f_k, cu $k < n$.

Avem $X_0 = \Omega_0 \cup X$. Condiția de morfism cere ca $f_0(\omega_{\tilde{X}}) = \omega_Q$ pentru orice $\omega \in \Omega_0$, în timp ce pentru $x \in X$ cerem ca $(\tilde{f} \circ i)(x) = f(x)$; ca atare trebuie ca $f_0(x) = f(x)$. Așadar, $f_0: \Omega_0 \to Q$ este definită și este unic determinată prin condițiile la care este supus $\tilde{f}$.

Presupunem că f_k este definit și unic determinat pentru $k < n$. Un element din X_n $(n \geqslant 1)$ este de forma $(\omega, a_1, \ldots, a_k)$, unde $\omega \in \Omega_k$, $a_i \in X_{m_i}$ și $\sum_{i=1}^{k} m_i = n-1$. Așadar, $f_{m_i}(a_i)$ este deja unic determinat pentru $i = 1, \ldots, k$. Apoi, deoarece $(\omega, a_1, \ldots, a_k) = \omega(a_1, \ldots, a_k)$ și cum proprietatea de morfism a lui $\tilde{f}$ cere ca $\tilde{f}(\omega, a_1, \ldots, a_k) = \omega(\tilde{f}(a_1), \ldots, \tilde{f}(a_k))$, trebuie să definim $f_n(\omega, a_1, \ldots, a_k) = \omega(f_{m_1}(a_1), \ldots, f_{m_k}(a_k))$. Prin aceasta f_n este bine determinat și cum fiecare element al lui $\tilde{X}$ aparține exact unei submulțimi X_n, punînd

$$\tilde{f}(z) = f_n(z) \quad \text{pentru} \quad z \in X_n, \quad n \geqslant 0,$$

rezultă că $\tilde{f}: \tilde{X} \to Q$ este un morfism de Ω-algebre, astfel încît $\tilde{f}(i(x)) = f_0(x) = f(x)$ pentru orice $x \in X$ și că $\tilde{f}$ este unic cu această proprietate. Teorema 3.2 este demonstrată. ∎

Observație. Sintetizăm demonstrația anterioară, presupunînd că X și Ω_0 sînt disjuncte (ceea ce se realizează renotînd etichetele din Ω_0). Considerînd că elementele acestor mulțimi sînt „cuvinte" (adică expresii formale finite care pot fi formate cu elemente din X și din Ω) și că pentru orice $\omega \in \Omega_n$, $n \geqslant 1$, dacă $w_1, \ldots, w_n$ sînt „cuvinte", atunci $w_1, \ldots, w_n\omega$ este de asemenea un „cuvînt", atunci $\tilde{X}$ este mulțimea tuturor „cuvintelor" obținute în acest mod. Aplicația $i: X \to \tilde{X}$, $x \mapsto x$ este evident injectivă. Structura de Ω-algebră pe $\tilde{X}$ este obținută definind aplicația $\tilde{\delta}: \Omega \to \operatorname{Op} \tilde{X}$ care asociază oricărei etichete ω cu $\nu(\omega) = n$, $n \geqslant 0$, operația n-ară $\tilde{X}^n \to \tilde{X}$, $(w_1, \ldots, w_n) \mapsto w_1 \ldots w_n \omega$. Este clar că $\forall\, \omega \in \Omega$, $\nu_{\tilde{X}}(\tilde{\delta}(\omega)) = \nu(\omega)$ căci dacă $\omega \in \Omega_n$, atunci $\nu_{\tilde{X}}(\tilde{\delta}(\omega)) = n$. În fine, pentru orice Ω-algebră (Q, δ) și oricare ar fi aplicația $f: X \to Q$ se consideră

$$\tilde{f}: \tilde{X} \to Q, \quad \tilde{f}(w) = \begin{cases} w & \text{dacă } w \in X, \\ \delta(w) & \text{dacă } w = w \in \Omega_0, \\ \delta(w)(w_1, \ldots, w_k) & \text{dacă } w = w_1 \ldots w_k\omega. \end{cases}$$

Într-un anumit sens, $\tilde{X}$ este „cea mai mică" Ω-algebră care conține X.

COROLAR. *Functorul ştergător*

$$\mathbf{U} : \Omega\text{-}\mathbf{alg} \to \mathbf{Set}$$

admite un adjunct şi pentru orice mulţime X, $\widetilde{X}$ *este o* Ω*-algebră liber generată de* X (în sensul definiţiei 3.7), *unică pînă la un izomorfism.*

Într-adevăr, cu notaţiile din definiţia 3.7, luăm $\mathbf{C} = \Omega\text{-}\mathbf{alg}$, $\mathbf{C}' = \mathbf{Set}$ şi $\forall X \in \mathrm{Ob}\,\mathbf{C}'$, $\mathbf{G}(\mathbf{X}) = \widetilde{X}$ şi $i_X : X \to \widetilde{X}$; teorema 3.2 arată că pentru orice $Q \in \mathrm{Ob}\,\mathbf{C}$ şi pentru orice aplicaţie de mulţimi $f : X \to Q$, există şi este unic un morfism $\tilde{f} : \widetilde{X} \to Q$ pentru care $\tilde{f} \circ i_X = f$, ceea ce trebuia demonstrat. ∎

Exemple. 1) Dacă $\Omega = \emptyset$ şi X este o mulţime oarecare, atunci $\widetilde{X} = X$.

2) Dacă $\Omega = \{*\}$ şi $\nu(*) = 1$, atunci pentru orice mulţime nevidă X rezultă $\widetilde{X} = X^*$, dicţionarul alfabetului X.

Un exemplu important este cuprins la punctul următor (algebra $\pi(X)$ a propoziţiilor peste o mulţime X).

Algebra propoziţiilor

Calculul propoziţional studiază modalităţile prin care din afirmaţii simple se pot forma afirmaţii mai complexe, cu conservarea criteriilor de adevăr. Dacă p şi q sînt propoziţii date, atunci se pot forma noi propoziţii: „p şi q", „p sau q", „non p", „p implică q" etc. Folosind cîteva elemente de algebră universală putem formaliza mai elegant astfel de construcţii, discutînd pe scurt problema adevărului (semantica) şi a demonstraţiei (sintactica) în calculul propoziţional.

Fie $\Omega = \{\mathbf{F}, \Rightarrow\}$ o signatură unde $\mathbf{F}$ este o etichetă de operaţie nulară („falsul"), iar „$\Rightarrow$" o etichetă de operaţie binară („implicaţia"). Orice Ω-algebră se numeşte *algebră de propoziţii.* Dacă X este o mulţime oarecare, se numeşte *algebră de propoziţii peste* X, Ω-algebra $\pi(X) = \widetilde{X}$ generată de X (există conform teoremei 3.2).

Exemplu. Corpul $\mathbb{B} = \mathbb{Z}_2$ este o Ω-algebră luînd $\mathbf{F} = 0$ şi $(m \Rightarrow n) = 1 + m + mn$.

În orice algebră de propoziţii vom introduce operaţiile derivate $\neg$, $\vee$, $\wedge$, $\equiv$, definite prin

$$\neg p = (p \Rightarrow \mathbf{F}); \; p \vee q = ((\neg p) \Rightarrow q); \; p \wedge q = \neg(\neg p \vee \neg q);$$

$$(p \equiv q) = ((p \Rightarrow q) \wedge (q \Rightarrow p)).$$

De exemplu, în $\mathbb{Z}_2$ avem $\neg p = 1 + p$, $p \vee q = p + q + pq$, $p \wedge q = pq$ şi $(p \equiv q) = 1 + p + q$.

Fie X o mulțime fixată (ale cărei elemente pot fi numite propoziții simple sau elementare). Atunci $\forall\, x \in X$, avem $x \in \pi(X)$. Apoi, dacă $x, y \in \pi(X)$, atunci $\neg x \in \pi(X)$, $(x \Rightarrow y) \in \pi(X)$. Se numește *funcție-valoare de adevăr* (sau *interpretare*) orice morfism de Ω-algebre

$$v : \pi(X) \to \mathbb{Z}_2.$$

O propoziție $p \in \pi(X)$ se spune că este *adevărată* (resp. *falsă*) relativ la v dacă $v(p) = 1$ (resp. $v(p) = 0$).

Orice funcție $X \to \mathbb{Z}_2$ se extinde, conform teoremei 3.2, la un morfism de Ω-algebre $\pi(X) \to \mathbb{Z}_2$. Deci este suficient să definim o interpretare v pentru elementele mulțimii X și atunci $v(p)$ este determinat pentru orice $p \in \pi(X)$.

Fie $A \subset \pi(X)$ o colecție de propoziții. Se spune că o propoziție $p \in \pi(X)$ este o *consecință* a lui A (sau că A *implică semantic* p) dacă ori de cîte ori v este o funcție-valoare de adevăr egală cu 1 pe A, are valoarea 1 și pentru p. Adică $v(q) = 1$, $\forall\, q \in A \Rightarrow v(p) = 1$. O propoziție $p \in \pi(X)$ se numește o *tautologie* (resp. o *contradicție*) dacă pentru orice interpretare v avem $v(p) = 1$ (resp. $v(p) = 0$). De exemplu, $(p \wedge q \Rightarrow p \vee q)$ este o tautologie iar $p \wedge \bar{p}$ este o contradicție.

Multe sisteme matematice sînt descrise prin seturi de axiome specifice. O demonstrație constă dintr-o succesiune de afirmații care se încheie cu proprietatea de demonstrat, fiecare din afirmații fiind dedusă din unele deja acceptate. Alegerea axiomelor și a regulilor de inferență (deducție) are adeseori motivații externe. Pentru calculul propozițional un set de axiome, scris foarte condensat, este următorul:

a) $\forall\, p, q \in \pi(X)$, $\quad p \Rightarrow (q \Rightarrow p)$;

b) $\forall\, p, q, r \in \pi(X)$, $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$;

c) $\forall\, p \in \pi(X)$, $\quad \neg(\neg p) \Rightarrow p$.

Toate aceste propoziții sînt tautologii, așa cum se verifică ușor. Ca unică regulă de inferență se consideră *modus ponens*:

$$\text{din } p \text{ și } p \Rightarrow q, \text{ se deduce } q.$$

Dacă $A \subset \pi(X)$ și $p \in \pi(X)$ se numește *demonstrație a lui* p *pornind de la* A orice șir finit $p_1, \ldots, p_n$ din $\pi(X)$ astfel încît $p_n = p$ și pentru orice $1 \leqslant i \leqslant n$ are loc una din situațiile următoare:

p_i este o axiomă sau aparține lui A; există $j, k < i$ astfel încît $p_k = (p_j \Rightarrow p_i)$. Dacă există o astfel de demonstrație, se mai spune că p este *demonstrabilă pornind de la* A (sau că A *implică sintactic* p).

O propoziție $p \in \pi(X)$ se numește *teoremă* a calculului propozițional peste X dacă p este demonstrabilă pornind de la $A = \emptyset$.

Un rezultat profund, demonstrat în ([2]), este următorul:

Dacă $A \subset \pi(X)$ este o colecție de propoziții și $p \in \pi(X)$, atunci p este o consecință a lui A dacă și numai dacă p este demonstrabilă pornind de la A (cu alte cuvinte, implicația semantică este echivalentă cu implicația sintactică sau mai sugestiv: o propoziție este adevărată dacă și numai dacă este demonstrabilă).

Nu intrăm în detalii și ne restrîngem la indicarea structurii laticiale pe mulțimea $\pi(X)$.

Se numește *latice* orice mulțime ordonată $(L, \leqslant)$ astfel încît $\forall\, a, b \in L$ există $a \wedge b = \inf\{a, b\}$ și $a \vee b = \sup\{a, b\}$. Se verifică ușor că pentru orice $a, b, c \in L$ avem:

1) $a \wedge a = a$, $a \vee a = a$ (idempotență);

2) $a \wedge b = b \wedge a$, $a \vee b = b \vee a$ (comutativitate);

3) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, $(a \vee b) \vee c = a \vee (b \vee c)$ (asociativitate);

4) $a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$ (absorbție).

O latice se numește *distributivă* dacă $\forall\, a, b, c \in L$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ și $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

O latice $(L, \leqslant)$ distributivă avînd un cel mai mic element $0 \in L$ (notat și $\bot$) un cel mai mare element, $1 \in L$ (notat și $\top$) și astfel încît $\forall\, a \in L$ există și este unic un element $\bar{a} \in L$ (notat uneori a' sau $\neg a$), cu proprietatea că $a \wedge \bar{a} = 0$, $a \vee \bar{a} = 1$, se numește *algebră Boole* (sau, echivalent, *latice booleană*).

Exemple. 1) Dacă X este o mulțime oarecare, atunci $\mathfrak{p}(X)$ este o latice booleană relativ la incluziune. Dacă $A, B \subset X$, atunci $\inf\{A, B\} = A \cap B$, $\sup\{A, B\} = A \cup B$, $0 = \emptyset$, $1 = X$ și $\forall\, A \subset X$, $\bar{A} = \complement A$.

2) Mulțimea $\mathbb{B} = \{0, 1\}$, ordonată prin $0 \leqslant 0$, $1 \leqslant 1$, $0 \leqslant 1$, este o latice booleană, relativ la $\vee$ și $\wedge$ uzuale ($0 \vee 0 = 0$, $0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1$; $0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0, 1 \wedge 1 = 1$), $\bar{0} = 1$, $\bar{1} = 0$.

3) Pentru orice mulțime X, algebra de propoziții $\pi(X)$ peste X este o algebră Boole relativ la implicație; în acest caz, $\forall\, p, q \in \pi(X)$, $p \wedge q = \inf\{p, q\}$, $p \vee q = \sup\{p, q\}$, $\bar{p} = \neg p$, $0 = \mathbf{F}$ (falsul), $1 = \neg \mathbf{F} = \mathbf{A}$ (adevărul).

De asemenea, mulțimea predicatelor unare relativ la o mulțime formează o algebră Boole (relativ la implicație).

Dacă $(L, \leqslant, \vee, \wedge, \neg, 0, 1)$ este o algebră Boole, atunci se poate considera aplicația $c : L^3 \to L$, punînd $c(x, y, z) = (x \wedge y) \vee (\bar{x} \wedge z)$, care definește o operație 3-ară pe L; în loc de $c(x, y, z)$ se mai scrie IF x THEN y ELSE z („dacă x atunci y altfel z"). Pentru orice $n \in \mathbb{N}$ și oricare ar fi aplicația $h : L^n \to L$, are loc relația

$$h(c(x, y_1, z_1), \ldots, c(x, y_n, z_n)) = c(x, h(y_1, \ldots, y_n), h(z_1, \ldots, z_n)),$$

pentru orice $x, y_i, z_i \in L$, $1 \leqslant i \leqslant n$.

Fie A o mulțime pe care sînt fixate două operații nulare 0 și 1 și o operație 3-ară $c : A^3 \to A$. 4-uplul $(A, c, 0, 1)$ se numește *algebră* ITE dacă $\forall\, x, y, z, u, v \in A$ au loc relațiile :

1) $c(c(x, y, z), u, v) = c(x, c(y, u, v), c(z, u, v))$;

2) $c(x, c(y, z, u), v) = c(y, c(x, z, v), c(x, u, v))$;

2′) $c(x, z, c(y, u, v)) = c(y, c(x, z, u), c(x, z, v))$;

3) $c(x, c(x, y, z), u) = c(x, y, u)$;

3′) $c(x, y, c(x, z, u)) = c(x, y, u)$;

4) $c(x, 1, 0) = x$;

5) $c(x, 0, 0) = 0$, $c(x, 1, 1) = 1$;

6) $c(0, x, y) = y$, $c(1, x, y) = x$.

Se verifică ușor că orice algebră Boole este o algebră ITE, punînd $c(x, y, z) = (x \wedge y) \vee (\overline{x} \wedge z)$; invers, dacă $(A, c, 0, 1)$ este o algebră ITE, atunci punînd

$$x \vee y = c(x, 1, y),\ x \wedge y = c(x, y, 0) \text{ și } \overline{x} = c(x, 0, 1),$$

se obține o algebră Boole. Această corespondență este bijectivă, deci calculul boolean este esențialmente echivalent cu calculul ITE.

Circuite logice

Se consideră circuitele logice elementare $x \mapsto \overline{x}$ (inversor); $(x, y) \mapsto x \wedge y$ (conjunctor); $(x, y) \mapsto x \vee y$ (disjunctor). Se numește *circuit logic* orice graf orientat în care vîrfurile sînt circuite elementare iar arcele — conductori. Mulțimea circuitelor logice are o structură de latice booleană : fie C_1, C_2 circuite logice ; $C_1 \vee C_2$ corespunde legării în serie, $C_1 \wedge C_2$ legării în paralel, $\overline{C}_1$ este inversatul lui C_1, $C_1 \leqslant C_2$ înseamnă $C_1 \wedge \overline{C}_2 = 0$.

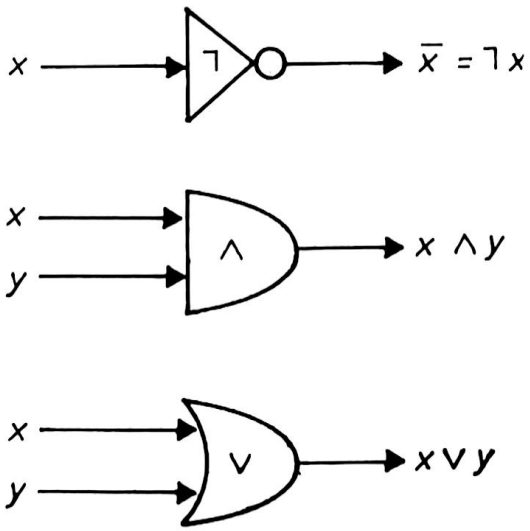


Fig. 3.6

Circuitul NAND (*not and*) al lui Sheffer și circuitul NOR (*not or*) al lui Pierce sînt indicate în fig. 3.7. Ele au proprietatea remarcabilă că orice circuit logic se poate realiza exclusiv cu NAND-uri (resp. cu NOR-uri). Într-adevăr, considerînd funcția Sheffer $\varphi : \mathbb{B}^2 \to$

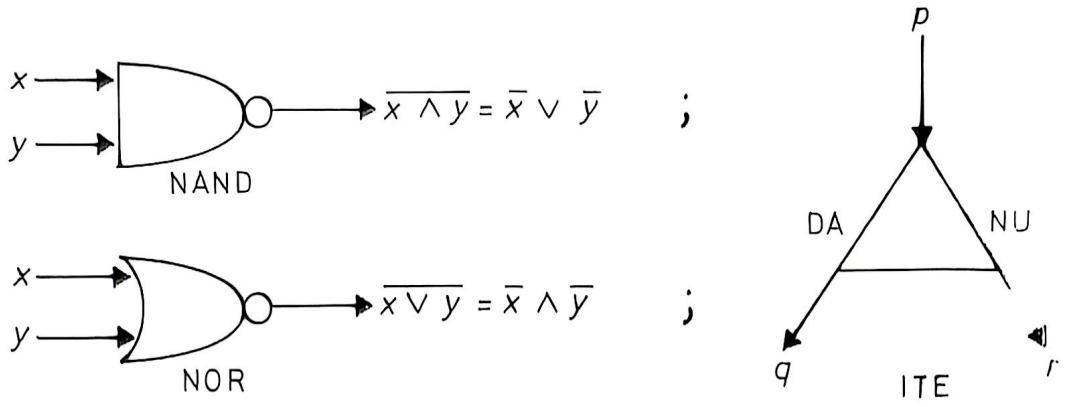


Fig. 3.7

$\to \mathbb{B}$, $\varphi(x, y) = \overline{x \wedge y}$, rezultă $\bar{x} = \varphi(x, x)$, $x \wedge y = \overline{\overline{x \wedge y}} = \overline{\varphi(x, y)} = \varphi(\varphi(x, y), \varphi(x, y))$ și $x \vee y = \overline{\bar{x} \wedge \bar{y}} = \overline{\varphi(x, x) \wedge \varphi(y, y)} = \varphi(\varphi(x, x), \varphi(y, y))$. Așadar, inversorii, conjunctorii și disjunctorii se realizează numai cu circuite NAND. În mod similar se raționează pentru funcția Pierce $\psi : \mathbb{B}^2 \to \mathbb{B}$, $\psi(x, y) = \overline{x \vee y}$.

De asemenea, se poate arăta că orice circuit logic se poate realiza numai cu circuitul $C =$ „if then else" (notat ITE în fig. 3.7). Anume, se pune $c(p, q, r) =$ if p then q else r, $\forall\, p, q, r \in \pi(X)$.

Pentru orice funcție-valoarea de adevăr $v : \pi(X) \to \mathbb{Z}_2$ se pune

$$v(c(p, q, r)) = \begin{cases} v(q) & \text{dacă } v(p) = 1, \\ v(r) & \text{dacă } v(p) = 0. \end{cases}$$

Avem
$\mathbf{F} =$ if p then $\bar{p}$ else $p = c(p, \bar{p}, p)$;
$(p \Rightarrow q) =$ if p then q else $\mathbf{A} = c(p, q, \mathbf{A})$, $\mathbf{A} = \neg\mathbf{F}$ fiind adevărul;
$(p \wedge q) =$ if p then q else $\mathbf{F} = c(p, q, \mathbf{F})$;
$\bar{p} =$ if p then $\mathbf{F}$ else $\mathbf{A} = c(p, \mathbf{F}, \mathbf{A})$,
deci circuitele logice elementare (și prin urmare toate celelalte) se pot realiza numai cu ajutorul lui $c =$ ITE.

Observație. Un rezultat interesant, datorat lui M. Stone afirmă că pentru orice latice booleană finită L există o mulțime finită X și o aplicație bijectivă $f : L \to \mathfrak{p}(X)$ astfel încît $\forall\, x, y \in L$, $f(x \vee y) = f(x) \cup f(y)$, $f(x \wedge y) = f(x) \cap f(y)$, $f(\bar{x}) = \mathbb{C}f(x)$ și $f(0) = \emptyset$, $f(1) = X$. O astfel de aplicație se mai numește un *izomorfism de latici*. Așadar, orice latice booleană (finită) este izomorfă cu laticea părților unei mulțimi. Acest rezultat se extinde la cazul infinit și arată de ce orice calcul logic boolean revine la un calcul folosind operațiile cu mulțimi.

§ 3.3. ARBORI ETICHETAȚI

Arbori ordonați

Reamintim că un graf orientat $G = (V, A, i, t)$ se numește arbore dacă există un vîrf distins $v_0 \in V$, numit rădăcina arborelui, astfel încît pentru orice vîrf $v \in V$ să existe și să fie unic un drum în G unind virfurile v_0 și v. Într-un arbore nu există drumuri închise de lungime $\geqslant 1$. Această noțiune apare curent în descrierea structurilor ierarhice.

Exemple. 1) În figura 3.8 pot fi vizualizate cîteva exemple de arbori.

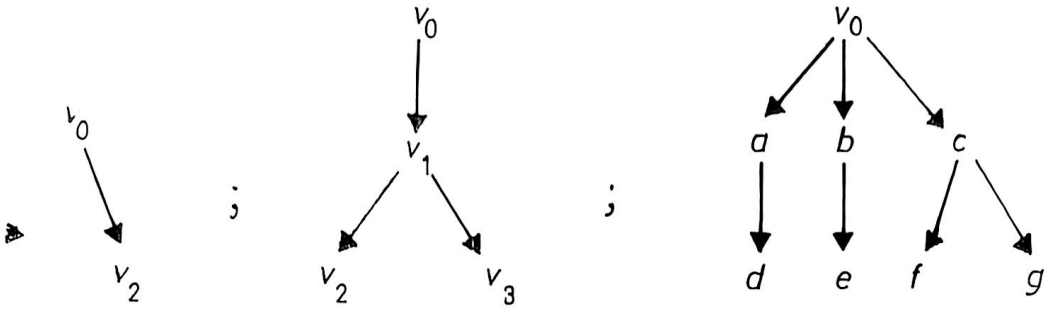


Fig. 3.8

2) Anumite relații de recurență sînt legate de structuri arborescente. De exemplu, șirul lui Fibonacci $\{a_n\}_{n \geqslant 0}$ este definit prin $a_0 = 1$, $a_1 = 1$ și $a_n = a_{n-1} + a_{n-2}$, $n \geqslant 2$. Pentru orice $n \geqslant 2$ se poate considera un arbore cu rădăcina a_n asociat acestui șir (fig. 3.9):

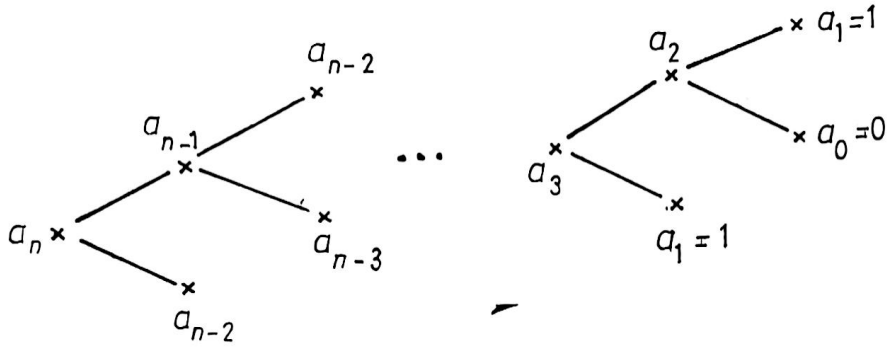


Fig. 3.9

3) Oricărei expresii aritmetice, algebrice sau logice i se poate asocia un arbore. De exemplu, expresiilor $a + a + (b \cdot c)$, $(p \wedge q) \vee p$ li se asociază arborii din fig. 3.10, în care

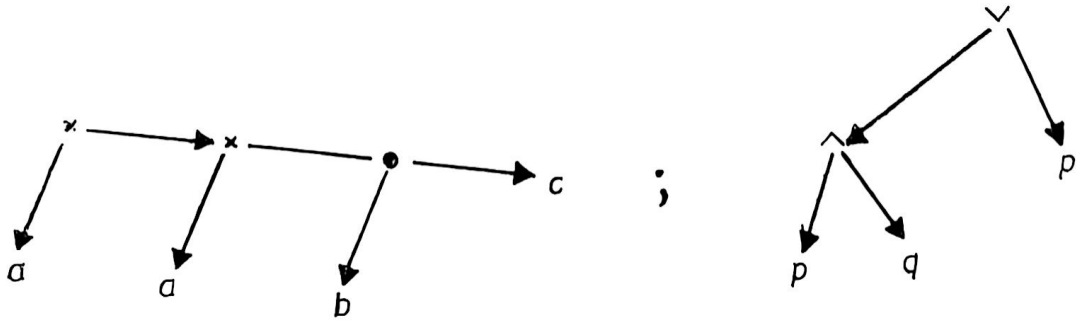


Fig. 3.10

vîrfurile sînt afectate cu simboluri de operații sau cu litere. Dar arborii din fig. 3.11 care constituie grafuri izomorfe corespund unor expresii algebrice distincte, anume a/bc și bc/a.

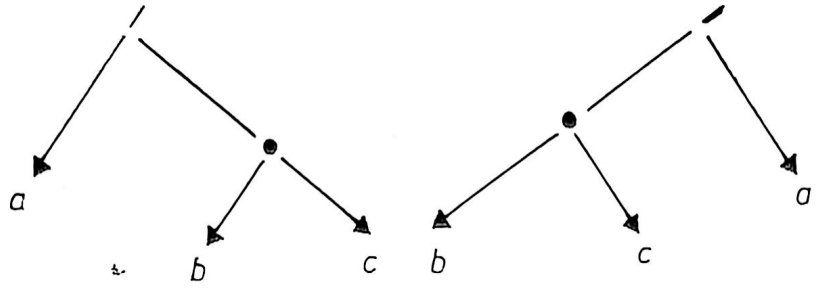


Fig. 3.11

Aceasta arată necesitatea unei ordonări a arcelor și justifică noțiunea următoare.

DEFINIȚIA 3.10. Se numește *arbore ordonat*, un arbore în care mulțimea vîrfurilor este o submulțime finită T a dicționarului $\mathbb{N}^*$ (colecția juxtapunerilor de numere naturale) astfel încît

1) $\wedge \in T$ ($\wedge$ este rădăcina);

2) de îndată ce $w \in \mathbb{N}^*$, $x \in \mathbb{N}$ și $wx \in T$, rezultă că $w \in T$ și $wy \in T$, pentru orice y cu $0 \leqslant y \leqslant x$.

Un astfel de arbore este notat pe scurt prin T. Așadar, T cuprinde cuvîntul vid și ori de cîte ori $w \in \mathbb{N}^*$, $0 \leqslant y \leqslant x$, $wx \in T$, rezultă $w \in T$ și $wy \in T$.

Dacă $wx \in T$, atunci se spune că wx este un *succesor* al lui w; dacă $w(n-1) \in T$ și $wn \notin T$, rezultă că w are n succesori, anume $w0, w1, \ldots, w(n-1)$. Un vîrf w al lui T se numește *terminal* (sau *frunză*) dacă $w0 \notin T$, adică w nu are succesori.

Exemple. 1) Luînd $T = \{\wedge, 3, 4, 31, 30, 42, 41, 40\}$ se obține un arbore ordonat, reprezentat în fig. 3.12. Acest arbore are cinci frunze, anume 30, 31, 40, 41, 42.

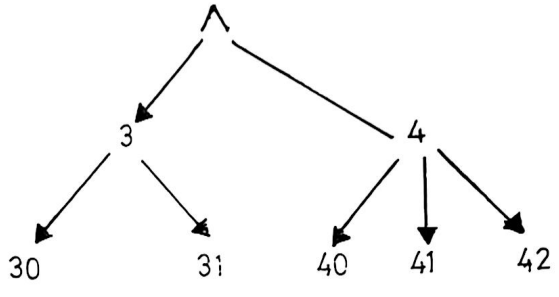


Fig. 3.12

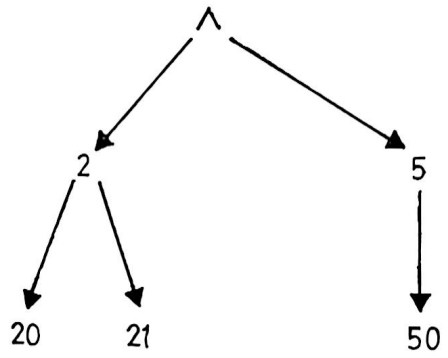


Fig. 3.13

2) Luînd $T = \{\wedge, 2, 5, 20, 21, 50\}$ se obține un arbore ordonat cu trei frunze, anume 20, 21, 50 (fig. 3.13).

De obicei prin drum într-un arbore se înțelege un drum care unește rădăcina cu oricare din vîrfurile terminale. Trebuie de ase-

menea remarcat că pentru orice arbore ordonat și pentru orice vîrf v există un subarbore al lui T avînd v ca rădăcină.

Pentru orice arbore ordonat T se poate defini o funcție

$$\nu_T : T \to \mathbb{N},\ w \to \text{numărul succesorilor lui } w.$$

Așadar,

$$\nu_T(w) = 1 + \max \{x \in \mathbb{N} \mid wx \in T\}$$

și $\nu_T(w) = 0$ dacă nu există $x \in \mathbb{N}$ astfel încît $wx \in T$.

Arbori etichetați

DEFINIȚIA 3.11. Fie (Ω, ν) o signatură. Se numește *arbore etichetat* (cu etichete din Ω) orice pereche (T, h) formată dintr-un arbore ordonat T (în sensul definiției 3.10) și o funcție de etichetare $h : T \to \Omega$ astfel încît

$$\forall\, w \in T,\ \nu(h(w)) = \nu_T(w),$$

adică orice vîrf w din T are o etichetă $h(w)$ și atîția succesori cît aritatea acestei etichete.

Exemplu. **Fie arborele $T = \{\wedge, 0, 1, 00, 01, 10, 11\}$ și signatura (Ω, ν) definită prin $\Omega = \{\oplus, \odot, \top\}$, $\nu(\oplus) = \nu(\odot) = 2$, $\nu(\top) = 0$. Definim funcția $h : T \to \Omega$,**

$$\begin{cases} h(\wedge) = \oplus,\ h(0) = \oplus,\ h(1) = \odot, \\ h(00) = h(01) = h(10) = h(11) = \top. \end{cases}$$

Se obține un arbore etichetat (indicat în fig. 3.14).

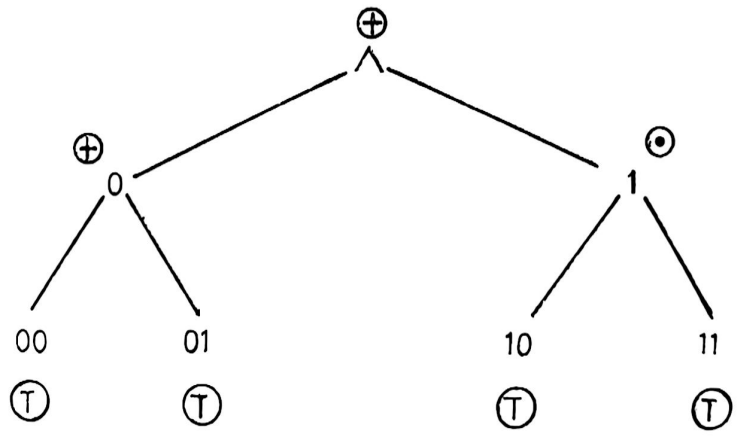


Fig. 3.14

Un rezultat remarcabil este cuprins în teorema următoare.

TEOREMA 3.3. *Fie (Ω, ν) o signatură. Mulțimea T_Ω a tuturor arborilor etichetați cu etichete din Ω este o Ω-algebră, care este obiect inițial în categoria Ω-algebrelor.*

Demonstrație. Definim mai întîi o aplicație

$$\delta_\Omega : \Omega \to Op\,(T_\Omega).$$

Fixăm $\forall\, \omega \in \Omega$, deci $\exists\, n \in \mathbb{N}$ astfel ca $\omega \in \Omega_n$, adică $\nu(\omega) = n$.

Dacă $n = 0$, atunci ω este etichetă de operație nulară și fixăm următorul element din T_Ω:

$T = \{\wedge\}$, cu eticheta ω; totodată punem $\delta_\Omega(\omega) = T$.

Dacă $n \geqslant 1$, atunci trebuie să asociem lui ω o operație n-ară pe mulțimea arborilor etichetați, cu etichete din Ω, adică să definim o aplicație

$$\delta_\Omega(\omega) : T(\Omega)^n \to T(\Omega).$$

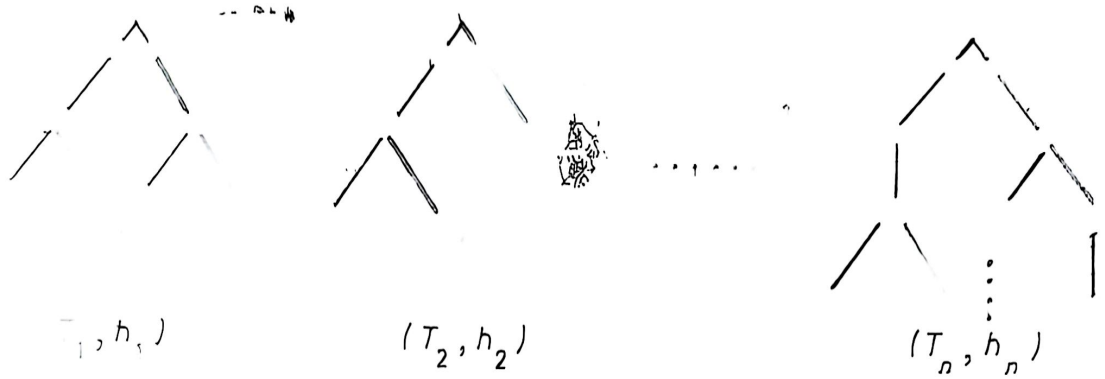


Fig. 3.15

Pentru aceasta avem de asociat oricăror n arbori etichetați (fig. 3.15), un alt arbore etichetat bine determinat. Anume, asociem arborele din fig. 3.16, unde vîrful $\wedge$ este etichetat tocmai cu ω care este etichetă

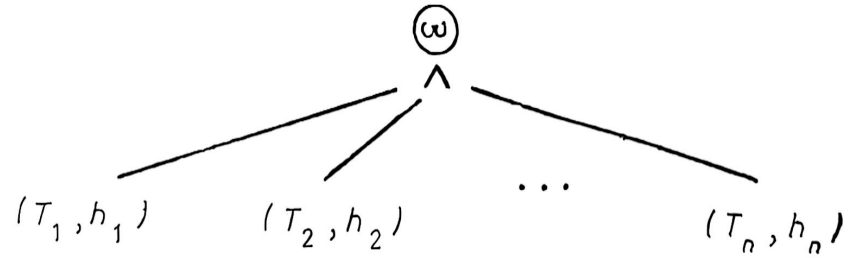


Fig. 3.16

de operație n-ară, iar inițialele arborilor sînt unite cu $\wedge$ și pot fi notate $0, 1, \ldots, n-1$ (în loc de $\wedge$).

Aplicația δ_Ω este definită. Rămîne să notăm că $\forall\, \omega \in \Omega$, aritatea operației $\delta_\Omega(\omega)$ este egală cu $\nu(\omega)$. Dar dacă $\nu(\omega) = n$, $n \geqslant 0$, atunci prin însăși definiția anterioară $\delta_\Omega(\omega)$ este o operație n-ară pe mulțimea T_Ω.

Rămîne să arătăm că T_Ω este obiect inițial în categoria Ω-alg. Într-adevăr, să observăm, urmărind demonstrația teoremei 3.2. că T_Ω este tocmai Ω-algebra generată de $\emptyset$, deci pentru orice Ω-algebră Q, pentru unica aplicație $\emptyset \to Q$ există un unic morfism $T_\Omega \to Q$. ■

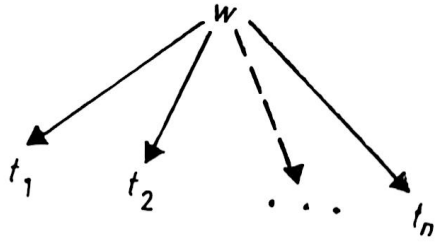
Evaluarea inductivă a arborilor etichetați

Fie Q o mulțime oarecare astfel încît $Q \cap \Omega = \emptyset$, ceea ce se obține renotînd elementele lui Ω. Extinzînd definiția 3.11, se numește *arbore etichetat peste* Q (cu etichete din Ω) orice pereche (T, h), unde T este un arbore ordonat și $h : T \to \Omega \cup Q$ este o funcție astfel încît:

1) $\forall w \in T$, cu $\nu_T(w) = n \geqslant 1$, să avem $h(w) \in \Omega_n$;

2) $\forall w \in T$, cu $\nu_T(w) = 0$, să avem $h(w) \in \Omega_0 \cup Q$.

Un arbore de tipul



se mai notează cu $w[t_1, \ldots, t_n]$. Atunci un arbore etichetat peste Q poate fi definit și prin inducție astfel:

— orice $w \in \Omega_0$ ca și orice $q \in Q$ este un arbore etichetat peste Q cu etichete din Ω (*baza de inducție*);

— dacă $t_1, \ldots, t_n$ sînt arbori etichetați peste Q și $\nu(w) = n$, atunci $w[t_1, \ldots, t_n]$ este un arbore etichetat peste Q (*pasul de inducție*).

Presupunem acum că (Q, δ) este o Ω-algebră cu signătura (Ω, ν) și că $Q \cap \Omega = \emptyset$; notăm că $T_{\Omega,Q}$ mulțimea arborilor etichetați peste Q (cu etichetele din Ω). Prin inducție pe arbori, se definește aplicația de evaluare

$$\delta^* : T_{\Omega,Q} \to Q$$

în modul următor:

— dacă $q \in Q$ este considerat un arbore, atunci $\delta^*(q) = q$, iar dacă $\nu(w) = 0$, se pune $\delta^*(w) = \delta(w) \in Q$ (*baza de inducție*);

— dacă $t_1, \ldots, t_n$ sînt arbori deja evaluați și dacă $\nu(w) = n$, atunci definim evaluarea lui $w[t_1, \ldots, t_n]$ punînd

$$\delta^*(w[t_1, \ldots, t_n]) = \delta(w)[\delta^*(t_1), \ldots, \delta^*(t_n)] \text{ (pasul de inducție).}$$

Observație. Notînd $\Omega_Q = \Omega \cup Q$ (reuniune disjunctă) și considerînd aplicația $\nu_Q : \Omega_Q \to \mathbb{N}$, $\nu_Q(z) = \begin{cases} \nu(z) & \text{dacă } z \in \Omega \\ 0 & \text{dacă } z \in Q, \end{cases}$ se obține o nouă signatură, (Ω_Q, ν_Q) căreia i se pot asocia arbori etichetați. Etichetele de operatori nulari sînt exact elementele din

$\Omega_0 \cup Q$, deci ele apar pe frunze, în timp ce orice alt vîrf w are $\nu(h(w))$ succesori. Teorema 3.3 se extinde astfel: *dacă* (Ω, ν) *este o signatură și* (Q, δ) *o* Ω*-algebră, atunci mulțimea* $T_{\Omega,Q}$ *a arborilor etichetați peste* Q *cu etichete din* Ω *este* Ω_Q*-algebra liberă generată de* Q.

§ 3.4. AUTOMATE; AUTOMATE-ARBORE

Automate în sens Eilenberg

Studiul matematic al automatelor este important pentru înțelegerea calculului programat și a modului de prelucrare a datelor pe dispozitive fizice. Un rol deosebit îl au automatele fără memorie sau capacitate de stocare a datelor, în legătură cu investigarea unor clase diferite de limbaje.

DEFINIȚIA 3.12. Fie X o mulțime nevidă fixată, numită *alfabet de intrare*. Se numește X*-automat* (sau *mașină deterministă*) orice 4-uplu

$$\mathcal{A} = (S, \delta, s_0, T)$$

alcătuit din următoarele entități:

1) o mulțime finită S (numită *mulțimea stărilor* automatului);

2) o aplicație $\delta : S \times X \to S$ (*funcția de tranziție* a stărilor);

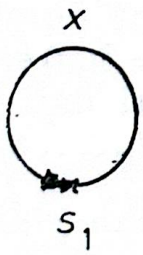
3) un element $s_0 \in S$ (*starea inițială*) și o submulțime de *stări terminale* $T \subset S$.

Trebuie remarcat că dacă $\mathcal{A} = (S, \delta, s_0, T)$ este un X-automat, atunci perechea (S, δ) este o X-dinamică în sensul definiției 1.13. De altfel, X-dinamicile, studiate în §1.5, se mai numesc uneori X-semiautomate.

Oricărui automat $\mathcal{A}$ i se poate asocia un graf orientat $G_{\mathcal{A}}$ în care vîrfurile sînt chiar stările automatului (elementele lui S) și două stări $s_1, s_2 \in S$ sînt unite printr-un arc dacă există o intrare $x \in X$ astfel încît $\delta(s_1, x) = s_2$; se mai scrie atunci

$$s_1 \xrightarrow{x} s_2 \text{ în cazul cînd } s_2 \neq s_1$$

și



în cazul cînd $s_2 = s_1$. Mulțimea A a arcelor grafului $G_{\mathcal{A}}$ apare astfel ca o submulțime de triplete din $S \times X \times S$. Despre un arc $\alpha = (p, x, q)$, notat și $p \xrightarrow{x} q$, se spune că *începe cu* p, *se termină cu* q

și *este etichetat cu* x. În conformitate cu definiția 3.1, $G_{\mathcal{A}}=(S, A, i, t)$, unde $i: A \to S$, $(p, x, q) \mapsto p$ și $t: A \to S$, $(p, x, q) \mapsto q$. În plus este definită o *funcție de etichetare*

$$l: A \to X, \ (p, x, q) \mapsto x.$$

Remarcăm că oricărui X-automat $\mathcal{A}$ având n stări $s_0, s_1, \ldots, s_{n-1}$ i se poate asocia o matrice pătratică de ordin n cu elemente din $\mathbf{p}(X)$, anume $[\tau_{pq}]_{0 \leqslant p,q \leqslant n-1}$, cu $\tau_{pq}=\{x \in X \mid (s_p, x, s_q)$, este un arc în $G_{\mathcal{A}}\}$. Se numește *drum* în X-automatul $\mathcal{A} = (S, \delta, s_0, T)$ unind stările s'_0, s'_k orice șir finit $(s'_0, x_1, x'_1), (s'_1, x_2, s'_2), \ldots, (s'_{k-1}, x_k, s'_k)$ de arce consecutive; numărul k este numit *lungimea drumului*. Un astfel de drum se mai notează

$$c = s'_0 \xrightarrow{x_1} s'_1 \xrightarrow{x_2} \ldots \xrightarrow{x_k} s'_k \text{ sau direct } c: s'_0 \to s'_k.$$

Se definește în mod natural *concatenarea* de drumuri.

DEFINIȚIA 3.13. Fie $\mathcal{A}= (S, \delta, s_0, T)$ un X-automat. Pentru orice drum $c: s'_0 \xrightarrow{x_1} s'_1 \xrightarrow{x_2} \ldots \xrightarrow{x_k} s'_k$ din A cuvîntul $x_1 x_2 \ldots x_k$ din dicționarul X^* se numește *eticheta* drumului c. Pentru orice $s \in S$ se introduce *drumul nul* $(s, \wedge, s)$ având eticheta $\wedge$. Se numește *drum reușit* în X-automatul $\mathcal{A}$ orice drum c care unește starea inițială $s_0 \in S$ cu o stare terminală (din T), adică $c: s_0 \to t$, cu $t \in T$. Mulțimea tuturor etichetelor de drumuri reușite în $\mathcal{A}$ este un limbaj în alfabetul X^* numit comportarea lui $\mathcal{A}$ și notat cu $|\mathcal{A}|$. Bineînțeles, submulțimea $\mathcal{A} \subset X^*$ nu se confundă cu „cardinalul automatului" $\mathcal{A}$.

Exemple de automate

1) Un atomat $\mathcal{A} = (S, \delta, s_0, T)$ în care $S = \emptyset$ se numește *automatul vid*. Dacă X este un alfabet oarecare și $x = x_1 \ldots x_n \in X^*, n \geqslant 1$, atunci se poate considera un automat cu $n + 1$ stări, $S = \{s_0, s_1, \ldots, s_n\}$, $T = \{s_n\}$ cu graful

$$s_0 \xrightarrow{x_1} s_1 \xrightarrow{x_2} \ldots \xrightarrow{x_n} s_n.$$

Aici există un singur drum reușit $c: s_0 \to s_n$ și $|\mathcal{A}| = \{c\}$.

2) Luînd $X = \{|\}$, $S = \{s_0, s'\}$, $T = S$, $\delta: S \times X \to S$, $(s_0, |) \mapsto s_0$; $(s', |) \mapsto s_0$ se obține un X-automat $\mathcal{A}$ al cărui graf asociat este indicat în fig. 3.17. Comportarea lui $\mathcal{A}$ este $\{\wedge, |, ||, |||, \ldots\}$ și se identifică cu $\mathbb{N}$.

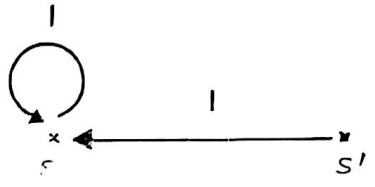


Fig. 3.17

3) Fie $X = \{a, b\}$, $S = \{s_0, s, s'\}$, $T = \{s, s'\}$ și $\delta: S \times X \to S$ definită prin tabloul

	a	b
s_0	s_0	s
s	s	s'
s'	s'	s'

adică $\delta(s_0, a) = s_0$, $\delta(s_0, b) = s$, $\delta(s, a) = s$, $\delta(s, b) = s'$, $\delta(s', a) = s'$, $\delta(s', b) = s'$. Graful asociat acestui automat este indicat în fig. 3.18.

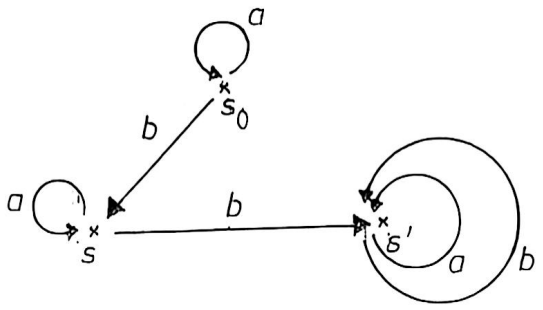


Fig. 3.18

Cuvinte acceptate, limbaje recunoscute

Fie X un alfabet (nevid). Vom vedea că orice X-automat $\mathcal{A} = (S, \delta, s_0, T)$ permite o clasificare a cuvintelor din dicționarul X^*. Mulțimea X joacă rolul de alfabet de intrare, literele sale fiind aplicate succesiv la momente discrete de timp. Fiecare literă din X provoacă o tranziție de stare; anume, dacă automatul se află în starea $s \in S$ și primește litera $x \in X$, atunci el trece în starea $\delta(s, x)$. Aplicînd la intrare o succesiune de litere (adică un cuvînt din X^*), se obține global tot o tranziție de stare ca efect cumulat al tranzițiilor determinate de fiecare literă în ordinea aplicării lor (adică ordinea în care literele figurează în cuvîntul considerat). Aplicînd cuvîntul vid, automatul rămîne în aceeași stare: $\delta(s, \wedge) = s$, $\forall\, s \in S$.

Vom presupune că înainte de aplicarea unui cuvînt automatul poate fi adus întotdeauna în starea inițială s_0 și că după aplicarea unui cuvînt putem stabili dacă automatul se află sau nu într-o stare terminală. Dacă $\mathcal{A}$ „pornește" din starea s_0 inițială și este dinamizat prin aplicația δ și dacă „primește" la intrare cuvîntul $c = x_1 x_2 \ldots x_k$ din X^*, de lungime $k \geqslant 1$, atunci pentru litera x_1 automatul trece în starea $s_1 = \delta(s_0, x_1)$; pentru litera x_2 el trece în starea $s_2 = \delta(s_1, x_2)$, apoi $s_3 = \delta(s_2, x_3)$ etc. Procesul continuă pînă ce este „citit" întreg cuvîntul c. Dacă starea finală s_k este terminală (adică din T), atunci cuvîntul c se numește *acceptat* (sau *recunoscut*) de automatul $\mathcal{A}$. Nu toate cuvintele din X^* sînt acceptate, ci evident numai cele care sînt etichete de drumuri reușite, deci cele aparținînd comportării lui $\mathcal{A}$. Mulțimea cuvintelor acceptate din X^* se mai numește *limbajul recunoscut* de automatul $\mathcal{A}$.

Se definește inductiv o funcție remarcabilă

$$\delta^* : S \times X^* \to S,$$

care asociază oricărei stări s și oricărui cuvînt $w \in X^*$ starea în care se va afla automatul după citirea cuvîntului w. Anume,

1) $\delta^*(s, \wedge) = s$ pentru orice $s \in S$ (*baza de inducție*). Dacă automatul pornește din starea s și primește la intrare cuvîntul vid, atunci el rămîne în starea s.

2) $\delta^*(s, wx) = \delta(\delta^*(s, w), x)$, $\forall\, s \in S$, $\forall\, w \in X^*$ și $\forall\, x \in X$ (*pasul de inducție*).

Atunci mulțimea cuvintelor acceptate de $\mathcal{A}$ este $\{w \in X^* \mid \delta^*(s_0, w) \in T\}$. Reținem deci că un X-automat poate să recunoască sau să respingă cuvintele din X^* : dacă primind un anumit cuvînt automatul ajunge din starea s_0 într-o stare terminală, atunci el este acceptat ; în caz contrar, cuvîntul este respins.

DEFINIȚIA 3.14. Fie X un alfabet finit. Un limbaj $L \subset X^*$ se numește *recognoscibil* (*în* X) dacă există un X-automat $\mathcal{A}$ astfel încît $L = |\mathcal{A}|$, adică L coincide cu comportarea unui X-automat. Orice astfel de X-automat se numește o *realizare* a limbajului L.

Așadar, L este recognoscibil dacă și numai dacă există un X-automat $\mathcal{A} = (S, \delta, s_0, T)$ astfel încît $L = \{w \in X^* \mid \delta^*(s_0, w) \in T\}$.

Se notează cu $\mathrm{Rec}\, X$ clasa limbajelor recognoscibile în X. Un rezultat fundamental în informatica teoretică și în studiul dinamicilor discrete îl constituie teorema lui Kleene care arată că limbajele recognoscibile sînt exact acele limbaje care se obțin folosind de un număr finit de ori așa-numitele operații raționale, plecînd de la cele mai simple limbaje. Vom da în capitolul 4 o extindere a acestei teoreme, obținînd totodată o aplicație remarcabilă în programarea structurată.

Observație. Pentru orice limbaj $L \subset X^*$ s-ar putea considera 4-uplul $(X^*, \delta, \wedge, L)$, unde $\delta : X^* \times X \to X^*$, $(w, x) \mapsto wx$ este X-dinamica Peano studiată în §1.5. Asimilînd X^* cu o mulțime de stări, $\wedge$ cu starea inițială și privind L ca mulțime de stări terminale, se observă că L apare ca mulțimea $\{w \in X^* \mid \delta^*(\wedge, w) \in L\}$. Totuși nu se obține o realizare a lui L pentru că 4-uplul anterior nu este un automat, deoarece are o infinitate de stări (cum $|X| \geqslant 1$, rezultă că mulțimea X^* este infinită). Or, dacă se urmărește „construirea" unui automat sau simularea funcționării lui pe calculator nu se poate accepta ideea infinității mulțimii stărilor acelui automat.

Exemple. 1) Fie $X = \{a, b\}$. Considerăm limbajele $L_1 = \{a^n \mid n \geqslant 0\}$, $L_2 = \{b^n \mid n \geqslant 0\}$ și fie $L = L_1 \cdot L_2 = \{a^m b^n \mid m \geqslant 0,\ n \geqslant 0\}$ concatenatul lor (definit în §1.4). Arătăm că $L \in \mathrm{Rec}\, X$. Într-adevăr, este suficient să considerăm X-automatul $\mathcal{A} = (S, \delta, s_0, T)$, unde $S = \{s_0, s_1, s_2\}$, $T = \{s_0, s_1\}$, cu graful indicat în fig. 3.19 și să observăm că $L = |\mathcal{A}|$.

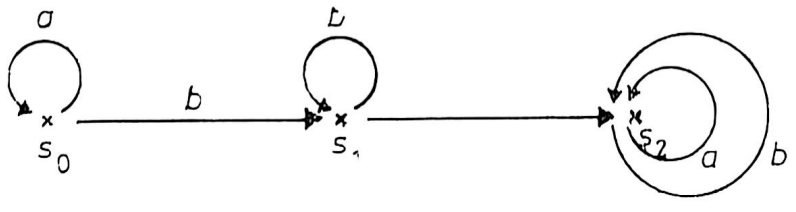


Fig. 3.19

2) Avem $\emptyset \in \mathrm{Rec}\, X$ pentru că alegem un X-automat $\mathcal{A} = (S, \delta, s_0, T)$, cu $T = \emptyset$. De asemenea, $1 = \{\wedge\} \in \mathrm{Rec}\, X$, pentru că alegem X-automatul $\mathcal{A} = (S, \delta, i, T)$, unde $S = \{s_0, s_1\}$, $T = \{s_0\}$; $\delta : S \times X \to S$, $\delta(s_0, \wedge_X) = s_0$, $\delta(s_1, \wedge_X) = s_1$. În acest caz. $|\mathcal{A}| = \{\wedge_X\}$.

3) Fie $X = \{a, b\}$. Arătăm că limbajul $L = \{a^n b^n \mid n \geqslant 1\}$ nu este recognoscibil în X. Într-adevăr, în caz contrar, cuvintele de forma $a^n b^n = \underbrace{a \ldots a}_{n \text{ ori}} \underbrace{b \ldots b}_{n \text{ ori}}$, $n \geqslant 1$ și numai ele ar fi acceptate de un X-automat $\mathcal{A} = (S, \delta, s_0, T)$, unde S este o mulțime finită. Presupunem că $|S| = k$ și considerăm mulțimea

$$S' = \{s_0, \delta^*(s_0, a), \delta^*(s_0, a^2), \ldots, \delta^*(s_0, a^k)\}.$$

Deoarece $S' \subset S$, deci $|S'| \leqslant |S|$, rezultă că există i, j $(0 \leqslant i < j \leqslant k)$ astfel încît $\delta^*(s_0, a^i) = \delta^*(s_0, a^j)$. Atunci

$$\delta^*(s_0, a^i b^j) = \delta^*(\delta^*(s_0, a^i), b^j) = \delta^*(\delta^*(s_0, a^j), b^j) = \delta^*(s_0, a^j b^j) \in T$$

(apartenența la T rezultă din ipoteza că $a^j b^j$ este acceptat de $\mathcal{A}$). Așadar, am arătat că $\mathcal{A}$ acceptă și cuvîntul $a^i b^j$, ceea ce este absurd, deoarece $i \neq j$.

Deoarece același limbaj poate avea mai multe realizări, se pune problema unei realizări „economice". Este deci necesară o ordonare a realizărilor unui același limbaj (de exemplu după cardinalul mulțimii stărilor). În acest scop, în lucrările de specialitate se dezvoltă conceptele de accesibilitate, observabilitate, realizare minimală ([13], [22]). Nu intrăm în detalii. Instrumentul principal pentru compararea automatelor îl constituie noțiunea de morfism.

Fie $\mathcal{A} = (S, \delta, s_0, T)$ și $\mathcal{A}' = (S', \delta', s_0', T')$ două X-automate. Se numește *morfism de X-automate* $f : \mathcal{A} \to \mathcal{A}'$ o aplicație $f : S \to S'$ astfel încît:

1) f să fie un morfism de X-dinamici $(S, \delta) \to (S', \delta')$;

2) $f(s_0) = s_0'$;

3) Pentru $s \in S$ avem $s \in T \leftrightarrow f(s) \in T'$ (adică $f(T) \subset T'$ și $f^{-1}(T') \subset T$).

Dacă între două X-automate $\mathcal{A}$ și $\mathcal{A}'$ există un morfism $f : \mathcal{A} \to \mathcal{A}'$, atunci se mai spune că $\mathcal{A}$ *simulează* $\mathcal{A}'$; în acest caz comportările lor coincid, $|\mathcal{A}| = |\mathcal{A}'|$. Verificarea este imediată. De asemenea, se verifică ușor că X-automatele și morfismele de X-automate formează o categorie.

Observație. În cele de mai sus am definit noțiunea de automat determinist. Se poate dezvolta și un concept de X-automat nedeterminist peste un alfabet X ca fiind un 4-uplu (S, δ, I, T) alcătuit dintr-o mulțime finită S de stări, o aplicație $\delta : S \times X \to \mathfrak{p}(S)$, care asociază oricărei stări $s \in S$ și oricărei intrări $x \in X$ mulțimea $\delta(s, x)$ a stărilor posibile, $I \subset S$ fiind mulțimea stărilor inițiale iar $T \subset S$ mulțimea stărilor finale.

Desigur, clasa limbajelor recognoscibile de X-automate nedeterministe este mai largă decît $\mathrm{Rec}\, X$.

Automate-arbore

DEFINIȚIA 3.15. Se numește *automat-arbore* un 6-uplu

$$\mathcal{A}_a = (\Omega, \nu, Q, \delta, Y, \beta)$$

alcătuit dintr-o signatură (Ω, ν), o Ω-algebră (Q, δ) astfel încît $\Omega \cap Q = \emptyset$, un alfabet de ieșire Y și o aplicație $\beta : Q \to Y$ numită *funcția de stare-ieșire.*

Automatele-arbore generalizează automatele deterministe. Anume, dacă (S, δ, s_0, T) este un X-automat în sensul definiției 3.12 și dacă se atașează o funcție stare-ieșire $\beta : S \to Y$, cu valori într-o mulțime Y, atunci se poate asocia un automat-arbore $(\Omega, \nu, Q, \delta_1, Y, \beta)$ în modul următor: se consideră $\Omega = X \cup \{\alpha\}$, unde $\alpha \notin X$; $\nu : \Omega \to \mathbb{N}$,

$$\nu(y) = \begin{cases} 1 \text{ dacă } y \in X \\ 0 \text{ dacă } y = \alpha \end{cases}; \quad Q = S \text{ și } \delta_1 : \Omega \to \operatorname{Op} Q, \text{ definită prin}$$

$$\delta_1(y) = \begin{cases} \text{operația unară } Q \to Q,\ s \mapsto \delta(s, y) & \text{dacă } y \in X, \\ \text{operația nulară pe } Q \text{ de fixare a stării } s_0 & \text{dacă } y = \alpha. \end{cases}$$

În același timp ele permit descrierea modului de realizare efectivă a operațiilor aritmetice, algebrice și logice, punct sensibil în intimitatea oricărui calculator modern.

Am văzut că dacă (Ω, ν) este o signatură și (Q, δ) este o Ω-algebră cu $\delta : \Omega \to \operatorname{Op} Q$, atunci se poate considera un arbore etichetat peste Q cu etichete din Ω, anume (T, h), unde T este un arbore ordonat și $h : T \to \Omega_Q = \Omega \cup Q$ este o funcție astfel încît orice vîrf w din T are $\nu_Q(h(w))$ succesori. Definim aplicația

$$\hat{h} : T \to Q$$

în modul următor: dacă $w \in T$ este un vîrf fixat, atunci se consideră elementul $h(w) \in \Omega \cup Q$ și apar trei cazuri:

1) $h(w) \in Q$; atunci punem $\hat{h}(w) = h(w)$;

2) $h(w) \in \Omega_0$ și punem $\hat{h}(w) = \delta(h(w)) \in Q$ (elementul din Q fixat prin operația nulară $\delta(h(w))$;

3) dacă $h(w) \in \Omega_n$, $n \geqslant 1$, atunci $\delta(h(w))$ este o operație n-ară $Q^n \to Q$ și se definește inductiv

$$\hat{h}(w) = \delta(h(w))(\hat{h}(w0), \hat{h}(w1), \ldots, \hat{h}(w(n-1)),$$

presupunînd că $\hat{h}$ a fost deja definită pentru vîrfurile w', cu $h(w') \in \Omega_{n-1}$ și acesta a fost cazul cu $w0, w1, \ldots, w(n-1)$. [De fapt,

aplicaţia $\hat{h}$ este legată de aplicaţia de evaluare δ^*; anume, $\forall\, T \in T_{\Omega,Q}$, $\hat{h}(\wedge) = \delta^*(T)$.]

Un automat-arbore asociază oricărui element din $T_{\Omega,Q}$ un element din Y numit *ieşirea* corespunzătoare; anume, se defineşte *funcţia-rezultat*

$$r : T_{\Omega,Q} \to Y, \quad (T, h) \mapsto \beta(\hat{h}(\wedge)).$$

Dacă $T \in T_{\Omega,Q}$ şi $\wedge$ este rădăcina arborelui T, atunci se calculează ca mai sus $\hat{h}(\wedge)$, care este un element din Q şi se aplică β acelui element. Se mai spune că funcţia r determină rezultatul acţiunii automatului-arbore $\mathcal{A}_a = (\Omega, \nu, Q, \delta, Y, \beta)$ pe arborii din $T_{\Omega,Q}$.

Exemple. 1) Fie automatul-arbore definit prin $\Omega = \{\oplus, \otimes\}$, $\nu : \Omega \to \mathbb{N}$, $\begin{matrix}\oplus \mapsto 2,\\ \otimes \mapsto 2,\end{matrix}$ $Q = \mathbb{N}$, $\delta : \Omega \to \mathrm{Op}\, Q$,

$\oplus \mapsto$ adunarea din $\mathbb{N}$

$\otimes \mapsto$ înmulţirea din $\mathbb{N}$, $Y = \mathbb{N}$ şi $\beta = 1_{\mathbb{N}}$. Considerăm arborele etichetat peste Q cu etichete din Ω indicat în fig. 3.20.

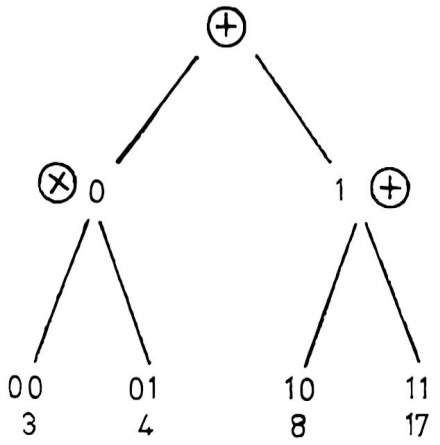


Fig. 3.20

Aşadar, $T = \{\wedge, 0, 1, 00, 01, 10, 11\}$ şi

$$h : T \to \Omega_Q = \Omega \cup Q, \quad \begin{matrix}\wedge \mapsto \oplus\\ 0 \mapsto \otimes;\\ 1 \mapsto \oplus\end{matrix} \quad \begin{matrix}00 \mapsto 3\\ 01 \mapsto 4\\ 10 \mapsto 8\\ 11 \mapsto 17\end{matrix}.$$

Neavînd etichete de operaţii nulare, pe frunze sînt marcate elemente din $Q = \mathbb{N}$, indicate în fig. 3.18. Rezultatul aplicării automatului anterior pe acest arbore este $\beta(\hat{h}(\wedge))$, adică $\hat{h}(\wedge)$. Dar $h(\wedge) \in \Omega_2$ deoarece $h(\wedge) = \oplus$, deci $\hat{h}(\wedge) = \hat{h}(\wedge 0) \oplus \hat{h}(\wedge 1) = \hat{h}(0) \oplus \hat{h}(1)$. Apoi, $h(0) = \otimes \in \Omega_2$ şi $\hat{h}(0) = \hat{h}(00) \otimes \hat{h}(01)$ şi cum $h(00) = 3 \in Q$, $h(01) = 4 \in Q$, rezultă $\hat{h}(00) = h(00) = 3$ şi, similar, $\hat{h}(01) = 4$. Ca atare, $\hat{h}(0) = 3 \otimes 4 = 12$. Pe de altă parte, $h(1) = \oplus \in \Omega_2$, deci $\hat{h}(1) = \hat{h}(10) \oplus \hat{h}(11)$ şi cum $h(10) = 8 \in Q$, $h(11) = 17 \in Q$, rezultă

$\hat{h}(10) = h(10) = 8$ şi $\hat{h}(11) = h(11) = 17$, deci $\hat{h}(1) = 8 \oplus 17 = 25$. În concluzie, $\hat{h}(\wedge) = 12 \oplus 25 = 37$.

Se subînţelege că rezultatul operaţiilor definite pe graful anterior se putea da imediat direct: $(3 \times 4) + (8 + 17) = 37$, dar chestiunea s-a pus la modul principal de descriere sistematică a modului de prelucrare a unui arbore etichetat printr-un automat-arbore.

2) Fie automatul-arbore definit prin entităţile următoare:

$$\Omega = \{x_2, x_3\}, \nu : \Omega \to \mathbb{N}, \quad \begin{matrix} x_2 \mapsto 2 \\ x_3 \mapsto 3 \end{matrix};$$

$$Q = \mathbb{R}, \delta : \Omega \to \mathrm{Op}\,\mathbb{R}, \quad \begin{matrix} x_2 \mapsto \text{înmulţirea a două numere reale} \\ x_3 \mapsto \text{înmulţirea a trei numere reale} \end{matrix};$$

$$Y = \mathbb{R} \text{ şi } \beta : \mathbb{R} \to \mathbb{R}, \quad x \mapsto \sin 2x.$$

Ne propunem să determinăm rezultatul acţiunii acestui automat pe arborele etichetat din fig. 3.21, pe frunzele căruia se află numerele reale π, a, b, c. Se verifică imediat că

$$\hat{h}(\wedge) = \hat{h}(0) \times \hat{h}(1) = \pi abc$$

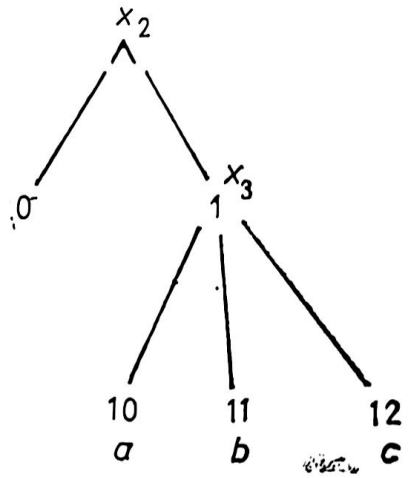


Fig. 3.21

şi rezultatul cerut este $\beta(\hat{h}(\wedge)) = \sin(2\pi abc)$.

§3.5. CALCULABILITATE

Ştiinţa calculului este un domeniu relativ recent în care s-au obţinut rezultate remarcabile prin care se fundamentează o teorie coerentă a sistemelor de calcul, legată mai mult sau mai puţin direct de realitatea fizică a calculatorului.

Sisteme iterative

Un calculator digital poate fi privit ca un obiect înzestrat cu o memorie şi cu posibilităţi de control asupra memoriei. De fapt, prin memorie se înţelege orice set de date care determină starea calcula-

torului la un moment dat, legată nu numai de stocarea informației, ci și de dispozitivele de intrare-ieșire sau de unele stări interne. În acest mod, un calculator poate fi descris printr-o mulțime S ale cărei elemente pot fi numite stări de memorie și printr-o funcție parțială $\varphi : S \to S$ corespunzînd instrucțiunilor de control. Desigur, descrierea structurii interne este aici grosieră; totuși ca o primă etapă este util conceptul introdus mai jos.

DEFINIȚIA 3.16. Se numește *sistem iterativ* orice pereche (S, φ) formată dintr-o mulțime S și o funcție parțială $\varphi : S \to S$.

Exemplu. Orice $\mathfrak{A}$-dinamică (în particular, mulțimea $\mathbb{N}$ împreună cu funcția-succesor) este un sistem iterativ.

Dacă (S, φ) este un sistem iterativ, un șir infinit $\{c_n\}_{n\geq 0}$ de elemente din S se numește *calcul în sistemul* (S, φ) dacă

1) $c_0 \in D_\varphi$ (domeniul de definiție al lui φ);

2) $\forall\, n \in \mathbb{N}, c_n \in D_\varphi$ și $c_{n+1} = \varphi(c_n)$.

Dacă există $i, j \in \mathbb{N}$, $0 \leqslant i < j$ și $c_i = c_j$, atunci $c_{i+m} = c_{j+m}$, $\forall\, m \in \mathbb{N}$ și calculul se numește *ciclic*. Un șir finit $c_0, \ldots, c_k$ de elemente din S se numește *calcul* dacă $c_0 \in D_\varphi$, $c_k \notin D_\varphi$ și pentru orice $0 \leqslant j < k$, $c_{j+1} = \varphi(c_j)$.

Se constată că în accepțiunea deterministă anterioară orice calcul este bine determinat de inițializarea c_0 presupusă din D_φ și îl notăm $\tilde{c}_0$; de asemenea, orice calcul are cel puțin doi termeni. Primul element al unui calcul se numește stare *inițială*, iar ultimul (în cazul unui calcul finit) stare *terminală*.

Dacă $(S, \varphi), (S', \varphi')$ sînt două sisteme iterative, se numește *morfism de simulare* de la primul la al doilea orice aplicație $s : S \to S'$ astfel încît $\forall\, x \in D_\varphi$ să avem $s(x) \in D_{\varphi'}$ și $\varphi'(s(x)) = s(\varphi(x))$. În acest caz, dacă $\tilde{c}_0$ este un calcul finit (resp. infinit sau ciclic) în sistemul iterativ (S, φ) avînd starea inițială c_0, atunci $\widetilde{h(c_0)}$ este un calcul de același tip în sistemul iterativ (S', φ').

Dacă (S, φ) este un sistem iterativ, prin subsistem iterativ al lui se înțelege orice sistem iterativ de forma (S_1, φ_1), unde $S_1 \subset S$ și $\varphi_1 = \varphi | S_1$.

O definiție a noțiunii de algoritm

Propunem acum o lărgire a conceptului de sistem iterativ și totodată o definiție pentru conceptul de algoritm. În limbajul uzual, prin algoritm se înțelege o procedură efectivă, definind un „șir de stări", numit calcul, avînd ca stare inițială un set de date de intrare și ca stare finală un anumit rezultat urmărit. În plus, procedura trebuie să fie deterministă (fiecare transformare de stare să fie definită fără ambiguitate), masivă (aplicabilă la o întreagă clasă de date

inițiale) și rezultativă (conducînd la rezultat după un număr finit de pași, în timp discret). Aplicarea unui algoritm revine la explicitarea unui șir de instrucțiuni privind îndeplinirea succesivă a unor operații asupra datelor inițiale. Cele spuse anterior reprezintă doar o circumscriere a conceptului de algoritm și totodată ne sugerează definiția următoare.

DEFINIȚIA 3.17. Vom numi *algoritm* un 6-uplu

$$\mathcal{A} = (S, I, T, \mathfrak{Q}, \mathfrak{R}, \tau),$$

unde :

— S este o mulțime finită (ale cărei elemente se numesc *stări*; ele pot fi seturi de date);

— $I \subset S$ (resp. $T \subset S$) este mulțimea stărilor *inițiale* (resp. *terminale*);

— $\mathfrak{Q}$ este o mulțime de predicate pe S (numite *condiții*);

— $\mathfrak{R}$ este o mulțime de relații binare pe S (numite *transformări de stare*);

— $\tau : \mathfrak{Q} \to \mathfrak{R}$ este o aplicație de mulțimi (funcția totală); pentru orice condiție $\pi \in \mathfrak{Q}$, $\tau(\pi)$ se numește transformarea de stare asociată lui π.

Deoarece S este finită, mulțimile I, T, $\mathfrak{Q}$, $\mathfrak{R}$ rezultă de asemenea finite (cap. 2, § 2.1). Orice condiție $\pi \in \mathfrak{Q}$ este o aplicație $\pi : S \to \mathbb{B}$ și orice transformare de stare $\rho \in \mathfrak{R}$ este o submulțime $\rho \subset S \times S$ (sau, cum se mai scrie, $\rho : S \to S$).

Fie $s_0 \in I$ o stare inițială. Apar două cazuri :

a) pentru orice $\pi \in \mathfrak{Q}$ avem $\pi(s_0) = 0$. Se consideră atunci că $s_0 \in T$, adică rezultatul este tot s_0 și algoritmul se oprește.

b) există $\pi \in \mathfrak{Q}$ (nu neapărat unic) astfel încît $\pi(s_0) = 1$. Se alege unul din aceste predicate și se aplică τ; fie $\rho = \tau(\pi) : S \to S$ transformarea de stare asociată lui π. Apar două subcazuri :

b_1) nu există $s \in S$ astfel încît $s_0 \rho s$ și atunci se consideră că $s_0 \in T$, iar algoritmul se termină.

b_2) există $s_1 \in S$ (nu neapărat unic) astfel încît $s_0 \rho s_1$ și pentru s_1 se reia procedeul aplicat anterior lui s_0 etc. Se constată că este acceptat un dublu nedeterminism.

Se obține un șir de stări

$$s_0, s_1, s_2, \ldots, s_n, \ldots$$

numit *calcul* realizat de algoritmul $\mathcal{A}$, începînd din starea s_0.

În general, dacă $\rho \in \mathrm{Rel}\, S$ este o relație binară pe S și notăm cu ρ^* închiderea reflexivă și tranzitivă a lui ρ, atunci se poate defini o nouă relație

$$\rho^{\top} = \{(s, t) \in \rho^* \mid t \notin D_\rho\}.$$

Faptul că $s\rho^{\top}t$ revine la aceea că s și t pot fi unite printr-un lanț de stări aflate două cîte două în relația ρ, care nu mai poate fi continuat la dreapta.

Dacă $\pi \in \mathfrak{P}$ este o condiție și $\rho_\pi = \tau(\pi)$ este transformarea de stare asociată, atunci vom introduce relația $\rho_\pi/\pi = \{(s, t) \in \rho_\pi | \pi(s) = 1\}$. Se numește *relație pe S calculată* de algoritmul $\mathcal{A}$, relația binară $R_{\mathcal{A}} = \bigcup_{\pi \in \mathfrak{P}} (\rho_\pi/\pi)^{\top}$. Așadar, sRt dacă și numai dacă există un calcul finit care începe cu s și se termină cu t. Așadar, $sRt \leftrightarrow \exists s_0, s_1, \ldots, s_n$ cu $s_0 = s$, $s_n = t$ și astfel încît oricare ar fi i, există $p_i \in \mathfrak{P}$ cu $p_i(s_i) = 1$ și $s_i \tau(p_i) s_{i+1}$.

Oricărui algoritm ca mai sus i se poate asocia un graf avînd S ca mulțime de vîrfuri. Drumurile care unesc o stare din I cu o stare din T se numesc drumuri *reușite*. Calculele finite sînt tocmai astfel de drumuri.

Într-o sinteză „formulizată",

$$\text{CALCUL} = \text{ALGORITM} + \text{DATE INIȚIALE},$$

la care se adaugă încă o formulă care va fi discutată în continuare:

$$\text{ALGORITM} = \text{MAȘINĂ} + \text{REGULI DE UTILIZARE}$$

(program realizat prin agenți).

Rămîne ca obiect de studiu ulterior încadrarea diverselor clase de procese calculatorii (funcții Turing-calculabile, funcțiile parțial recursive, algoritmi Markov normali, gramatici etc.) în definiția 3.17, ca și studiul dinamicii de tip nedeterminist propusă cu acest prilej.

Funcții aritmetice

Dacă $f : X \to Y$ este o funcție parțială, atunci vom nota cu $\chi_f : X \to \mathbb{N}$ funcția caracteristică a domeniului D_f de definiție al lui f,

$$\chi_f(x) = \begin{cases} 1 & \text{dacă } x \in D_f, \\ 0 & \text{dacă } x \in X \setminus D_f. \end{cases}$$

DEFINIȚIA 3.18. Se numește *funcție aritmetică* de m variabile, orice funcție parțială

$$f : \mathbb{N}^m \to \mathbb{N}^n \text{ (cu } m, n \geqslant 0).$$

Noțiunea de funcție aritmetică nu este cîtuși de puțin una particulară. Pentru prelucrarea și transmiterea oricăror informații, nu neapărat numerice, se folosesc alfabete finite convenabile de simboluri. Dacă A este un astfel de alfabet, atunci A^* este mulțime numă-

rabilă și există o aplicație bijectivă $A^* \xrightarrow{\varphi} \mathbb{N}$. Procesele respective de prelucrare și transmitere sînt descrise prin funcții $(A^*)^m \to (A^*)^n$; prin bijecția φ care revine la o numerotare convenabilă a simbolurilor din A, orice astfel de funcție este esențialmente echivalentă cu o funcție aritmetică.

În stadiul actual al dezvoltării teorici calculabilității, chiar dacă nu s-a reușit încă elaborarea unui concept suficient de general și unanim acceptat de algoritm, s-au obținut rezultate profunde relativ la descrierea unei clase importante de funcții aritmetice, anume funcțiile calculabile. În 1936 A. Church a conjecturat că orice funcție calculabilă are valorile calculabile cu ajutorul unei mașini și reciproc. Această teză este confirmată experimental, verificată în multe contexte teoretice particulare, dar nu poate avea statut de teoremă generală, întrucît nu toți termenii utilizați pot fi definiți ansamblist, independent de ideea de program. Înainte de a da definiții precise vom începe cu o discuție euristică pregătitoare. Prin „program" vom înțelege un program pentru un calculator universal, fără limitări de timp sau de memorie și avînd la îndemînă un spațiu special de blancuri unde pot fi inserate valori ale argumentelor funcțiilor calculabile.

Fixăm un element notat simbolic $\top$ care nu aparține nici unei mulțimi $\mathbb{N}^m$, $m \geqslant 0$. O funcție aritmetică $f : \mathbb{N}^m \to \mathbb{N}^n$ se numește *intuitiv calculabilă* (resp. *semicalculabilă*) dacă există un program care pentru orice $x \in \mathbb{N}^m$ determină la ieșire elementul $f(x)$ în cazul cînd $x \in D_f$, iar în cazul cînd $x \notin D_f$ programul determină $\top$ (resp. determină $\top$ sau lucrează fără oprire). Este evident că orice funcție intuitiv calculabilă este intuitiv semicalculabilă și reciproc dacă funcția este totală.

Fie $f : \mathbb{N}^m \to \mathbb{N}^n$ o funcție aritmetică și $\chi_f : \mathbb{N}^m \to \mathbb{N}$ funcția caracteristică a lui D_f. Demonstrăm următoarele afirmații:

1) *Dacă f este intuitiv semicalculabilă, atunci f este intuitiv calculabilă dacă și numai dacă χ_f este intuitiv calculabilă.*

Într-adevăr, dacă f este intuitiv calculabilă, atunci χ_f este intuitiv calculabilă pentru că la programul care calculează f adăugăm instrucțiunea „trimite $\top$ în 0 și orice element diferit de $\top$ în 1, apoi tipărește". Invers, dacă f este intuitiv semicalculabilă și dacă χ_f este intuitiv calculabilă, atunci înaintea programului de semicalcul al lui f se pune programul care calculează χ_f și apoi se adaugă instrucțiunea de a da $\top$ la ieșire de îndată de $\chi_f(x) = 0$ și de a continua programul pentru f avînd x ca argument, de îndată ce $\chi_f(x) = 1$.

2) *Funcția f este intuitiv calculabilă dacă și numai dacă f și χ_f sînt intuitiv semicalculabile.*

Într-un sens afirmația rezultă direct din cea anterioară. Reciproc, presupunem că f și χ_f sînt intuitiv semicalculabile. Atunci χ_f fiind totală este intuitiv calculabilă și aplicînd afirmația 1) rezultă că f este intuitiv calculabilă.

Afirmația secundă arată că este suficient de formalizat noțiunea de semicalculabilitate. Convenim să numim *necalculabilă* o funcție aritmetică ce nu este intuitiv semicalculabilă. Deoarece orice program este un limbaj finit într-un alfabet finit, mulțimea tuturor programelor este numărabilă. Așadar, mulțimea funcțiilor intuitiv semicalculabile este numărabilă, în timp ce mulțimea tuturor funcțiilor aritmetice este nenumărabilă (există o aplicație injectivă $\mathbb{B}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$, deci $|\mathbb{N}^{\mathbb{N}}| \geqslant |\mathbb{R}| > \aleph_0$). Prin urmare există funcții necalculabile.

Teza lui Church (versiunea slabă) afirmă că este posibil să fie indicată o familie de funcții aritmetice de bază intuitiv semicalculabile și o familie de operații elementare care aplicate la funcții intuitiv semicalculabile să genereze alte funcții de acest tip și, în plus, orice funcție intuitiv semicalculabilă să poată fi obținută din funcțiile aritmetice de bază printr-un număr finit de aplicări ale operațiilor elementare.

În discuția anterioară nu am precizat termenul de program și am dorit numai să pregătim terenul pentru prezentarea conceptului de funcție parțial recursivă, una din marile invenții ale secolului al XX-lea, legată de numele lui K. Gödel, S. Kleene,

A.M.Turing și al românului G.Sudan. Acest concept constituie ingredientul oricărei teorii a algoritmilor, deoarece reprezintă modelul matematic al noțiunii de funcție calculabilă.

DEFINIȚIA 3.19. Se numesc *funcții aritmetice de bază* următoarele funcții :

1) $s : \mathbb{N} \to \mathbb{N}$, $x \mapsto x + 1$ (*funcția succesor*) ;

2) $0_n : \mathbb{N}^n \to \mathbb{N}$, $(x_1, \ldots, x_n) \mapsto 0$, $\forall\, n \geqslant 0$ (*funcția nulă*) ;

3) $p_i^n : \mathbb{N}^n \to \mathbb{N}$, $(x_1, \ldots, x_n) \mapsto x_i$, $\forall\, n \geqslant 1$, $1 \leqslant i \leqslant n$ (*funcțiile-proiecție*).

Definim următoarele patru operații elementare cu funcțiile aritmetice (parțiale) :

a) *Compunerea.* Dacă $f : \mathbb{N}^m \to \mathbb{N}^n$ și $g : \mathbb{N}^n \to \mathbb{N}^p$, atunci se definește funcția compusă $g \circ f : \mathbb{N}^m \to \mathbb{N}^p$, unde $D_{g \circ f} = \{x \in \mathbb{N}^m \mid x \in D_f$ și $f(x) \in D_g\}$ și $\forall\, x \in D_{g \circ f}$, $(g \circ f)(x) = g(f(x))$.

Orice număr $k \in \mathbb{N}$ definește o funcție constantă $\mathbb{N}^n \to \mathbb{N}$, $(x_1, \ldots, x_n) \mapsto k$. Anume $\overbrace{s \circ \ldots \circ s}^{k \text{ ori}} \circ 0_n$.

b) *Juxtapunerea.* Să considerăm r funcții aritmetice

$$f_1 : \mathbb{N}^m \to \mathbb{N}^{p_1}, \ldots, f_r : \mathbb{N}^m \to \mathbb{N}^{p_r}$$

având același număr de variabile m. Se poate defini funcția aritmetică

$$f : \mathbb{N}^m \to \mathbb{N}^{p_1 + \ldots + p_r}, \text{ unde } D_f = D_{f_1} \cap \ldots \cap D_{f_r},\ f(x) = (f_1(x), \ldots, f_r(x)).$$

c) *Recursia primitivă.* Fie $f : \mathbb{N}^m \to \mathbb{N}$ și $g : \mathbb{N}^{m+2} \to \mathbb{N}$. Atunci se poate considera funcția parțială $h : \mathbb{N}^{m+1} \to \mathbb{N}$ definită prin inducție după ultimul argument prin

$$h(x_1, \ldots, x_m, 0) = f(x_1, \ldots, x_m) ;\ h(x_1, \ldots, x_m, k + 1) =$$

$$= g(x_1, \ldots, x_m, k, h(x_1, \ldots, x_m, k)) \text{ pentru } k \geqslant 0.$$

Domeniul de definiție D_h al lui h este de asemenea definit prin inducție

$$(x_1, \ldots, x_m, 0) \in D_h \leftrightarrow (x_1, \ldots, x_m) \in D_f ;$$

$$(x_1, \ldots, x_m, k + 1) \in D_h \leftrightarrow (x_1, \ldots, x_m, k) \in D_h \text{ și } (x_1, \ldots, x_m,$$

$$k, h(x_1, \ldots, x_m, k) \in D_g$$

pentru orice $k \geqslant 0$. Funcția aritmetică h se numește *recursia primitivă* a lui f și g ; se mai notează $h = \mathcal{R}(f, g)$.

Este remarcabil că operațiile de compunere, juxtapunere și recursie primitivă aplicate la funcții aritmetice totale conduc tot la funcții totale. Nu același lucru se întîmplă cu operația de minimizare descrisă mai jos.

d) *Minimizarea.* Fie $f(x_1, \ldots, x_n, x_{n+1})$, $f : \mathbb{N}^{n+1} \to \mathbb{N}$ o funcție aritmetică de $n + 1$ variabile. Atunci se poate considera funcția

$g : \mathbb{N}^n \to \mathbb{N}$ de n variabile pentru care

$$D_g = \{(x_1, \ldots, x_n) \in \mathbb{N}^n \mid \exists\, x_{n+1} \geqslant 0 \text{ astfel ca } f(x_1, \ldots, x_n, x_{n+1}) = 0 \text{ și } (x_1, \ldots, x_n, k) \in D_f \text{ pentru orice } k \leqslant x_{n+1}\}$$

și $g(x_1, \ldots, x_n) = \min\{x_{n+1} \in \mathbb{N} \mid f(x_1, \ldots, x_n, x_{n+1}) = 0\}$. Funcția g astfel definită se numește *minimizata* lui f (în raport cu ultima variabilă).

Funcții primitiv recursive, funcții parțial recursive

DEFINIȚIA 3.20. Fie $f : \mathbb{N}^m \to \mathbb{N}^n$ o funcție aritmetică totală. Ea se numește *primitiv recursivă* dacă există un șir (nu neapărat unic) de funcții aritmetice totale $f_1, \ldots, f_p = f$, numit *descriere primitiv recursivă* a lui f astfel încît f_1 să fie una din funcțiile aritmetice de bază și pentru orice $2 \leqslant k \leqslant p$, f_k să fie sau o funcție aritmetică de bază sau să fie obținută prin aplicare de operații elementare de compunere, juxtapunere sau recursie primitivă funcțiilor $f_1, \ldots, f_{k-1}$.

O funcție aritmetică (parțială sau totală) $f : \mathbb{N}^m \to \mathbb{N}^n$ se numește *parțial recursivă* dacă există un șir de funcții aritmetice $f_1, \ldots, f_p = f$, numit *descriere parțială recursivă* a lui f, astfel încît f_1 să fie una din funcțiile aritmetice de bază și pentru orice $2 \leqslant k \leqslant p$, f_k să fie sau o funcție de bază sau să fie obținută prin aplicare succesivă de operații elementare (compunere, juxtapunere, recursie primitivă sau minimizare) funcțiilor $f_1, \ldots, f_{k-1}$.

Exemplu. Funcția-sumă $\sigma : \mathbb{N}^2 \to \mathbb{N}$, $(x, y) \mapsto x + y$ este primitiv recursivă, deoarece avem descrierea primitiv recursivă

$$p_1^1, s, p_3^3, g = s \circ p_3^3, \ \sigma = \mathcal{R}(p_1^1, g).$$

În mod similar, funcția-produs $\pi : \mathbb{N}^2 \to \mathbb{N}$, $(x, y) \mapsto xy$ este primitiv recursivă, deoarece $\pi = \mathcal{R}(f, g)$, unde $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto 0$ și $g : \mathbb{N}^3 \to \mathbb{N}$, $(x_1, x_2, x_3) \mapsto x_1 + x_3$.

Evident, orice funcție primitiv recursivă este parțial recursivă. G. Sudan a dat un exemplu de funcție parțial recursivă totală care nu este primitiv recursivă, care a făcut obiectul unor cercetări remarcabile ale matematicienilor români C. Calude, S. Marcus, I. Tevy ([11], [30]).

Teza lui Church (versiunea tare) este următoarea : o funcție aritmetică f este semicalculabilă dacă și numai dacă ea este parțial recursivă ; f este calculabilă dacă și numai dacă f și χ_f sînt parțial recursive ; nu am precizat însă definițiile semicalculabilității și calculabilității, care nu pot fi date în afara precizării unui concept de program.

În sprijinul tezei lui Church, trebuie să observăm că funcțiile de bază trebuie să fie calculabile, oricare ar fi accepția termenului, iar prin aplicarea operațiilor elementare unor funcții semicalculabile se obțin tot funcții semicalculabile, un program pentru calculul acestora obținîndu-se din programele care calculează funcțiile originale. Partea nebanală a tezei lui Church este inversa : funcțiile semicalculabile sînt parțial recursive. Așa cum am mai spus, acest fapt a fost verificat doar experimental, în lipsa unui concept de calculabilitate independent de ideea de program sau, mai bine spus, atît timp cît nu am formalizat încă însuși procesul de calcul (de exemplu, clasa funcțiilor semicalculabile prin mașina Turing, cu specificul respectiv, coincide cu clasa PR ([6]) ; în aceeași ordine de idei demonstrăm teorema 3.5).

Mașina funcțiilor parțial recursive; limbajul LOOP

Să notăm cu PR clasa funcțiilor parțial recursive. Ne punem problema descrierii unei „mașini" care pentru orice funcție $f \in$ PR de m variabile (m arbitrar) și $\forall (x_1, \ldots, x_m) \in D_f$ să poată calcula $f(x_1, \ldots, x_m)$. În acest sens va fi esențial că PR este generată pornind de la funcțiile aritmetice de bază, prin mecanismele primare de generare oferite de operațiile elementare (compunere, juxtapunere, recursie primitivă, minimizare). Dacă mașina calculează valorile funcțiilor de bază și „știe" să efectueze cele patru operații elementare, atunci este evident că mașina va putea calcula valorile oricărei funcții din PR. Descrierea parțial recursivă a unei funcții $f \in$ PR este, așa cum am văzut, un șir neunic de funcții aritmetice (legat de o structură arborescentă), care începe cu o funcție de bază și se încheie cu f. Acest șir poate fi numit un program π_f pentru calculul valorilor lui f pe mașina considerată. Mașina atinge aici un prim nivel de universalitate : avînd programul π_f înregistrat în memorie, mașina poate calcula $f(x_1, \ldots, x_m)$ pentru *orice* date inițiale $x_1, \ldots, x_m$ admisibile (adică $(x_1, \ldots, x_m) \in D_f$). Dacă se modifică f, atunci și programul se modifică. Reținem deci că dacă mașina are un program π_f și un set de date inițiale, atunci ea oferă calculul valorii corespunzătoare a lui f. Nu se poate spune că mașina „execută" un program și aici apare un element extramatematic — *procesorul*, capabil să interpreteze programul, să citească datele inițiale, să efectueze calculul și a cărui inteligență depinde de tehnologie. Trebuie remarcat că orice funcție deja calculată poate fi luată la rîndul ei ca funcție de bază (înmagazinare de cultură!).

Calculul se face prin schimbări succesive de stări, prin stare la un moment t înțelegîndu-se aici mulțimea valorilor semnificative (aflate în memorie) la momentul t. Dacă calculul valorii lui f într-un punct se realizează în k pași, atunci el este un șir de $k + 1$ stări. Asocierea $f \mapsto$ numărul de pași în care se calculează valoarea lui f într-un punct admisibil nu este bine definită și depinde de asemenea de tehnologie.

Vom prezenta acum un limbaj de programare, numit LOOP, descoperit de Minsky și Ritchie, echivalent ca putere de calcul cu clasa funcțiilor primitiv recursive. Prin construcții similare conceptual dar introducînd instrucțiuni suplimentare de tip CONTINUE, se pot indica limbaje de programare echivalente cu clasa funcțiilor parțial recursive (în spiritul confirmării tezei lui Church) ([6], [11]). Sînt necesare cîteva pregătiri.

În general pentru a defini un limbaj de programare sînt necesare indicarea alfabetului simbolurilor utilizate pentru a construi programe corecte și explicitarea mulțimii programelor corecte, odată

cu „înțelesul" acestora. Dacă L este un limbaj avînd o mulțime infinită de cuvinte (relativ la un alfabet fixat), este dificilă numerotarea elementelor lui L și o metodă importantă de specificare a cuvintelor constă în utilizarea gramaticilor generative [(34]). O gramatică constă dintr-o mulțime de reguli numite producții care precizează sintaxa limbajului, structura cuvintelor. În limbajul uzual structura unei fraze este descrisă prin subiect, predicat etc.; tot astfel, structura unui program este dată în termeni de proceduri, propoziții, expresii etc. Gramatica ne permite să decidem printr-o procedură efectivă dacă o propoziție aparține sau nu unui anumit set de propoziții corecte, ca și analiza relațiilor între propoziții.

Notăm cu T o mulțime nevidă de simboluri *terminale* și cu N o mulțime de simboluri *neterminale*, cu $T \cap N = \emptyset$. Se numește *gramatică* orice triplet (N, T, G), unde G este o submulțime finită,

$$G \subset \{(n, w) | n \in N \text{ și } w \in (N \cup T)^*\}$$

ale cărei elemente se numesc *producții*; pentru o producție $(n, w) \in G$ se mai scrie $n \to w$. Dacă $w_1, w_2 \in (N \cup T)^* \setminus \{\wedge\}$, atunci se scrie $w_1 \Rightarrow w_2$ (și uneori $w_1 = w_2$, citindu-se „w_1 devine w_2") și se spune că w_2 *derivă direct* din w_1, ori de cîte ori există $\alpha, \beta \in (N \cup T)^*$, eventual vide, astfel încît $w_1 = \alpha A \beta$, $w_2 = \alpha p \beta$ și $A \to p$.

Exemplu. Se poate lua $T = \{a, b\}, N = \{A\}, G = \{A \to aAb, A \to \wedge\}$.

Relația „$\Rightarrow$" de derivare directă este o relație binară pe mulțimea $(N \cup T)^* \setminus \{\wedge\}$. Închiderea ei reflexivă și tranzitivă se notează „$\overset{*}{\Rightarrow}$" și se numește *relația de derivare*. Faptul că $w_1 \overset{*}{\Rightarrow} w_2$ înseamnă că sau $w_2 = w_1$ sau există $c_1, \ldots, c_k \in (N \cup T)^* \setminus \{\wedge\}$, $k \geqslant 1$, astfel încît $w_1 = c_1$, $c_1 \Rightarrow c_2, \ldots, c_{k-1} \Rightarrow c_k$ și $c_k = w_2$.

Exemplu. În exemplul anterior, $A \overset{*}{\Rightarrow} aabb$ deoarece $A \Rightarrow aAb \Rightarrow aaAbb \Rightarrow aabb$.

Ori de cîte ori există un neterminal într-un cuvînt din $(N \cup T)^*$, se poate *produce* un nou cuvînt. Dar dacă un cuvînt conține numai terminale, atunci nu se pot produce noi cuvinte, adică derivarea încetează.

Dacă fixăm N, T, G iar $s \in N$ este un simbol neterminal, atunci cuvintele derivate din s avînd toate literele simboluri terminali se numesc *programe* și mulțimea lor $L_s(G)$ se numește *limbajul generat* de gramatica (N, T, G) și de simbolul s. Așadar, $L_s(G) = \{u \in T^* | s \overset{*}{\Rightarrow} u\}$. Dacă (N, T, G) este o gramatică, atunci se poate defini un algoritm $\mathcal{A} = (S, I, T, \mathfrak{Q}, \mathfrak{R}, \tau)$ în sensul definiției 3.17, luînd $S \subset (N \cup T)^*$ finită, $I = N$, $T =$ mulțimea terminalelor, $\mathfrak{Q} =$ mulțimea funcțiilor caracteristice ale limbajelor $L_s(G)$, cu $s \in N$, $\mathfrak{R} =$ mulțimea relațiilor pe S, $\tau : \mathfrak{Q} \to \mathfrak{R}$, $L_s(G) \to$ relația de derivare asociată lui s.

Observație. Dacă (N, T, G) este o gramatică, atunci pentru orice simbol neterminal $S \in N$ se pot considera arbori de derivare avînd rădăcina în S, iar $L_S(G)$ este mulțimea cuvintelor obținute prin concatenarea literelor aflate pe frunzele arborilor respectivi. În exemplul anterior, am văzut că $A \overset{*}{\Rightarrow} aabb$ (anume, $A \Rightarrow aAb \Rightarrow aaAbb \Rightarrow aabb = a^2b^2$) și, de asemenea, $A \overset{*}{\Rightarrow} aaabbb$ (căci $A \Rightarrow aAb \Rightarrow aaAbb \Rightarrow aaaAbbb \Rightarrow aaabbb = a^3b^3$); arborii respectivi sînt indicați în fig. 3.22. Prin calcul direct rezultă $L_A(G) = \{a^n b^n \mid n \in \mathbb{N}\}$.

Dacă există un singur neterminal, atunci există o corespondență bijectivă între cuvintele limbajului generat și arborii asociați (și se mai spune că gramatica este neambiguă).

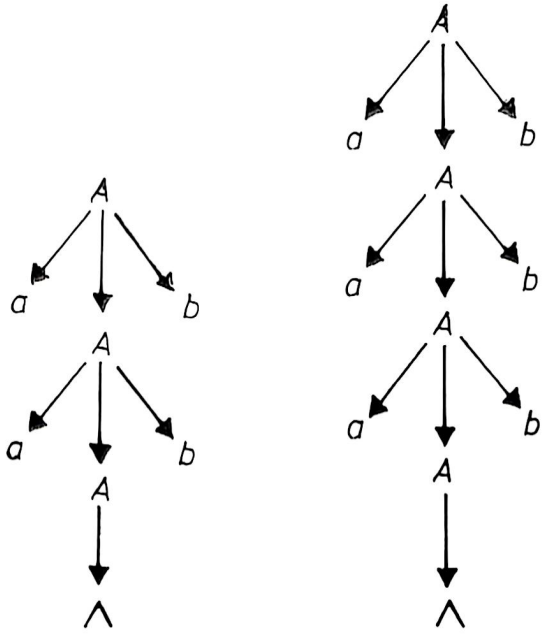


Fig. 3.22

Cu aceste pregătiri, fie V o mulțime numărabilă, liniar ordonată ($\leqslant$) numită mulțimea variabilelor LOOP. Limbajul LOOP este generat de o gramatică cu un singur simbol neterminal notat ⟨prog⟩, cu $T = \{clear, incr, move, \leftarrow, (, ;, :), loop, end\} \cup V$ avînd o mulțime numărabilă de producții. Pentru a simplifica sintaxa, notăm aceste producții cu π_α; acestea sînt

π_0	: ⟨prog⟩ = $\wedge$ (cuvîntul vid)	aritate 0
$\pi_{1,v}$	: ⟨prog⟩ = *clear* v, $\forall\, v \in V$	aritate 0
$\pi_{2,v}$	: ⟨prog⟩ = *incr* v, $\forall\, v \in V$	aritate 0
$\pi_{3,v,v'}$	: ⟨prog⟩ = *move* $v \leftarrow v'$ $(v, v' \in V)$	aritate 0.

În aceste producții partea dreaptă conține numai terminale. Se adaugă producțiile

π_4	: ⟨prog⟩ = (⟨prog⟩ ; ⟨prog⟩)	aritate 2
$\pi_{5,v}$	: ⟨prog⟩ = *loop* v : ⟨prog⟩ *end*, $\forall\, v \in V$	aritate 1.

Fiecare producție $\pi_0, \pi_1, \pi_2, \pi_3$ generează programe, iar π_4, π_5 generează programe pornind de la programe. Mulțimea π a producțiilor este în mod natural o signatură, cu aritățile indicate (aritatea este

determinată de numărul de apariții în membrul drept a simbolului neterminal). Se obține o gramatică

$$(N, T, G), \text{ unde } N = \{\langle \text{prog} \rangle\} \text{ și } G = \{\pi_0, \pi_{1,v}, \pi_{2,v}, \pi_{3,v,v'},$$

$$\pi_4, \pi_{5,v} \mid v, v' \in V\}.$$

Vom nota cu $P \subset T^*$ mulțimea programelor LOOP asociate, adică limbajul generat de gramatica de mai sus (cuprinzînd șiruri finite de simboluri terminale).

TEOREMA 3.4. *Mulțimea P are o structură de π-algebră, care este obiect inițial în categoria π-algebrelor.*

Demonstrație. Oricărui simbol de operator nular din signatura π îi asociem cîte un program, anume partea dreaptă a producției respective. Pentru operatorul binar, unei perechi (p, q) de elemente din P i se asociază programul $p\,;q$. Producția π_4 permite programe de tip $p\,;q\,;r$ care reprezintă o ambiguitate sintactică negravă (ce corespunde semantic unei reguli de asociativitate). În fine, pentru orice $v \in V$ avem cîte un simbol de operație unară de tip $\pi_{5,v}$ și îi asociem programul corespunzător din membrul drept. Se obține astfel o π-algebră. Faptul că P este un obiect inițial în categoria π-**alg** este datorat neambiguității gramaticii. Așadar, pentru orice π-algebră Q în care operația π_4 este asociativă, există și este unic un morfism $P \xrightarrow{\theta} Q$. ∎

Astfel, orice π-algebră Q ca mai sus este un domeniu semantic pentru programele LOOP și morfismul θ asociază oricărui program obiectul semantic care constituie un „înțeles" pentru el. Reținem că a da o semantică LOOP revine la a fixa o π-algebră.

Organizăm mulțimea $\mathbf{p}(V)$ ca π-algebră astfel:

π_0 : $\emptyset \in \mathbf{p}(V)$;

$\pi_{1,v}$: $\{v\} \in \mathbf{p}(V)$;

$\pi_{2,v}$: $\{v\} \in \mathbf{p}(V)$;

$\pi_{3,v,v'}$: $\{v\} \cup \{v'\} \in \mathbf{p}(V)$;

π_4 : $\mathbf{p}(V) \times \mathbf{p}(V) \to \mathbf{p}(V)$, $(A, B) \mapsto A \cup B$;

$\pi_{5,v}$: $\mathbf{p}(V) \to \mathbf{p}(V)$, $A \mapsto A \cup \{v\}$.

Morfismul unic de π-algebre var : $P \to \mathbf{p}(V)$ transformă orice program p în mulțimea variabilelor care figurează în p.

Vom indica acum principalul domeniu semantic, mai precis o π-algebră care poate fi descrisă în termenii unei mașini (numită mașina LOOP).

Luăm ca spațiu de stări (sau configurații) ale mașinii LOOP $S = \mathbb{N}^V$ și ca mulțime a transformărilor de stare ale mașinii $\mathcal{T} = S^S$; așadar, S are puterea continuului și orice stare a mașinii este o asignare de numere naturale — variabilelor (fiind o funcție $V \to \mathbb{N}$). Organizăm mulțimea $\mathcal{T}$ ca π-algebră în modul următor:

$\pi_0 : 1_S : S \to S, 1_S \in \mathcal{T}$;

$\pi_{1,v}$: *clear* $v \in T$ [aplicația $S \to S$, $\varphi \mapsto \psi$, ce lasă pe loc variabilele cu excepția lui v care este înlocuită cu 0; anume, se asociază oricărei funcții $\varphi \in \mathbb{N}^V$ funcția $\psi \in \mathbb{N}^V$, $\psi(w) = \begin{cases} \varphi(w) & \text{dacă } w \neq v \\ 0 & \text{dacă } w = v \end{cases}$];

$\pi_{2,v} : incr\ v \in \mathcal{T}$ (aplicația $S \to S$, $\varphi \mapsto \psi$, care asociază oricărei funcții $\varphi \in \mathbb{N}^V$ funcția $\psi \in \mathbb{N}^V$, $\psi(w) = \begin{cases} \varphi(w)+1 & \text{dacă } w = v \\ \varphi(w) & \text{dacă } w \neq v \end{cases}$;

$\pi_{3,v,v'} : move\ v, v'$ (aplicația $S \to S$, $\varphi \mapsto \psi$, care asociază oricărei funcții $\varphi \in \mathbb{N}^V$ funcția $\psi \in \mathbb{N}^V$, $\psi(w) = \begin{cases} \varphi(v') & \text{dacă } w = v \\ \varphi(w) & \text{dacă } w \neq v \end{cases}$;

$\pi_4 : S^S \times S^S \to S^S, (t, t') \mapsto t' \circ t$ este compunerea;

$\pi_{5,v}$: *loop* v ($\forall\, v \in V$, aceasta este funcția $S^S \to S^S$, $t \mapsto t'$, unde $t' : S \to S$, $s \mapsto t^{s(v)}(s)$).

$\mathcal{T}$ fiind o π-algebră, conform teoremei 3.4, există un singur morfism de π-algebre $\mathrm{tr} : P \to \mathcal{T}$, care asociază oricărui program p, transformarea de stare $\mathrm{tr}(p)$ asociată.

Așadar, să imaginăm o mașină (abstractă) alcătuită dintr-o memorie împărțită în celule corespunzînd variabilelor din V. Aceste celule pot conține numere naturale. *O stare* (sau o *configurație*) a mașinii este o funcție $s : V \to \mathbb{N}$. Execuția unui program p pe această mașină se realizează ca o transformare de stare $\mathrm{tr}(p)$ a mașinii.

Dăm o listă de proprietăți legate de entitățile introduse mai sus:

1) *orice π-subalgebră a lui P coincide cu P.*

Fie $Q \subset P$ o π-subalgebră și $j : Q \to P$ morfismul de incluziune. Conform teoremei 3.4, există un morfism unic $\theta : P \to Q$. Considerînd morfismul de π-algebre $j \circ \theta : P \to P$ și folosind din nou teorema 3.4 rezultă $j \circ \theta = 1_P$, deci aplicația j este surjectivă și $Q = P$.

Observație. Această proprietate reprezintă un „principiu de inducție pe programe": adeseori în practică se arată că mulțimea de adevăr a unui anumit predicat este o subalgebră.

Dăm acum cîteva proprietăți semantice ale programelor.

2) $\forall\, p \in P$, *mulțimea* $\mathrm{var}\, p$ *este finită*;

3) $\forall\, p \in P$, $\forall\, s \in S$, *aplicațiile* s *și* $\mathrm{tr}(p)(s)$ *coincid pe mulțimea* $V \setminus \mathrm{var}(p)$;

Din proprietăţile 2), 3) rezultă proprietatea următoare de *finitudine locală* a programelor. Acest rezultat are şi o valoare filozofică deoarece stabileşte care sînt stările „active", interesante, răspunzînd totodată şi întrebării critice: ce caută un spaţiu de stări de puterea continuului într-o teorie esenţialmente discretă?

4) *Fie* $\tilde{S} = \{s \in S \mid s(v) = 0$ pentru toate variabilele v cu excepţia unui număr finit$\}$. *Atunci pentru orice* $p \in P$, $\mathrm{tr}\,(p)(\tilde{S}) \subset \tilde{S}$.

Aşadar, programele conservă finitudinea locală a stărilor. Rezultă totodată că se pot considera ca stări doar elementele lui $\tilde{S}$ care formează doar o mulţime numărabilă.

Funcţiile calculabile de programele LOOP

Pentru orice $m, n \in \mathbb{N}$ vom numi (m, n)-*selecţie intrare-ieşire* (sau selecţie a m variabile de intrare şi n variabile de ieşire) orice pereche ordonată $(\bar{x}, \bar{y})$, cu $\bar{x} \in V^m$ şi $\bar{y} \in V^n$.

Orice element $\bar{z} \in V^k$, $\bar{z} = (z_1, \ldots, z_k)$ $(k \in \mathbb{N})$ se poate identifica prin proiecţia $\bar{z} : S = \mathbb{N}^V \to \mathbb{N}^k$, $s \mapsto (s(z_1), \ldots, s(z_k))$. În cazul special $k = 0$ avem $V^0 = \{\wedge\}$, $\mathbb{N}^0 = \{0\}$ şi atunci $\wedge : S \to \mathbb{N}^0$, $s \mapsto 0$.

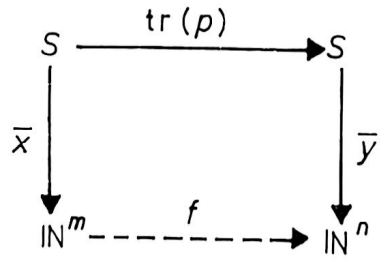
O selecţie $(\bar{x}, \bar{y})$ se numeşte *funcţională* pentru un program $p \in P$ dacă

$$\forall\, s, s' \in S,\ \bar{x}(s) = \bar{x}(s') \Rightarrow \bar{y}(\mathrm{tr}\,(p)(s)) = \bar{y}(\mathrm{tr}\,(p)(s')).$$

Cu alte cuvinte, dacă stările coincid în datele iniţiale (adică au aceleaşi valori pe intrări), atunci ele au aceleaşi valori şi după ieşire.

Exemplu. **Selecţia $(\overline{x}, \wedge)$ este funcţională în raport cu orice program. Apoi, pentru orice $p \in P$, selecţia $(\overline{\mathrm{var}\,p}, \mathrm{var}\,p)$ este funcţională.**

În cazul cînd o selecţie $(\bar{x}, \bar{y})$ este funcţională pentru un program $p \in P$, există şi este unică o funcţie aritmetică totală $f : \mathbb{N}^m \to \mathbb{N}^n$, notată $f = [\bar{x}, p, \bar{y}]$, făcînd comutativă diagrama următoare:



Funcţia f se numeşte *funcţia calculată de programul* p *prin selecţia funcţională* $(\bar{x}, \bar{y})$.

Funcţiile aritmetice $f : \mathbb{N}^m \to \mathbb{N}^n$ pentru care există p şi $(\bar{x}, \bar{y})$ ca mai sus, astfel ca $f = [\bar{x}, p, \bar{y}]$ se numesc *funcţii* LOOP-*calculabile*.

LEMA 1. *Fie* $\varphi : V \to V$ *o bijecție și definim* $\psi : \Sigma \to \Sigma$, $\psi(w) = \begin{cases} \varphi(w) & \text{dacă } w \in V \\ 1 & \text{dacă } w \notin V \end{cases}$, unde $\Sigma = T \cup N$. *Considerînd morfismul indus* $\psi^* : \Sigma^* \to \Sigma^*$ (strict alfabetic), *avem* $\psi^*(P) \subset P$. *În plus, pentru orice selecție* $(\bar{x}, \bar{y})$ *funcțională pentru* $p \in P$ *avem* $[\varphi(\bar{x}), \psi^*(p), \overline{\varphi(\bar{y})}] = [\bar{x}, p, \bar{y}]$.

Lema 1 exprimă invarianța funcțiilor calculate relativ la „redenumirea" variabilelor. De aici rezultă că orice funcție LOOP-calculabilă poate fi calculată utilizînd variabile din afara unei mulțimi finite date de variabile. Anume, dacă $A \subset V$ este o mulțime finită, p este un program și $(\bar{x}, \bar{y})$ este o selecție funcțională pentru p, astfel încît p calculează f prin $(\bar{x}, \bar{y})$, atunci există un program p' și o selecție funcțională $(\bar{x}', \bar{y}')$, astfel încît p' calculează f prin aceasta și $(\text{var}(p') \cup \bar{x}' \cup \bar{y}') \cap A = \emptyset$. Așadar, orice funcție calculată se poate calcula și fără a folosi variabile dintr-o mulțime finită dată.

LEMA 2. *Clasa funcțiilor primitiv recursive* (definiția 3.18) *coincide cu clasa funcțiilor aritmetice totale care conține funcțiile*

$$\alpha : \mathbb{N} \to \mathbb{N}^0,\ n \mapsto 0\ ;\ \beta : \mathbb{N}^0 \to \mathbb{N},\ 0 \mapsto 0 \text{ (am notat } \mathbb{N}^0 = \{0\})\ ;$$

$$1_{\mathbb{N}} : \mathbb{N} \to \mathbb{N},\ n \mapsto n\ ;\ s : \mathbb{N} \to \mathbb{N},\ n \mapsto n + 1$$

și este închisă relativ la operațiile de compunere $(g \circ f)$, *combinație* $(f \times g)$ *și exponențiere* [pentru orice funcție $f : \mathbb{N}^k \to \mathbb{N}^k$, $k \geqslant 1$, se definește *exponențierea lui* p ca fiind funcția $f^* : \mathbb{N}^k \times \mathbb{N}^k \to \mathbb{N}^k$, $(x, n) \mapsto f^n(x)$].

Demonstrația este directă.

Rezultatul principal al acestui paragraf îl constituie.

TEOREMA 3.5 (*Minsky-Ritchie*). *Orice funcție primitiv recursivă este* LOOP-*calculabilă și reciproc.*

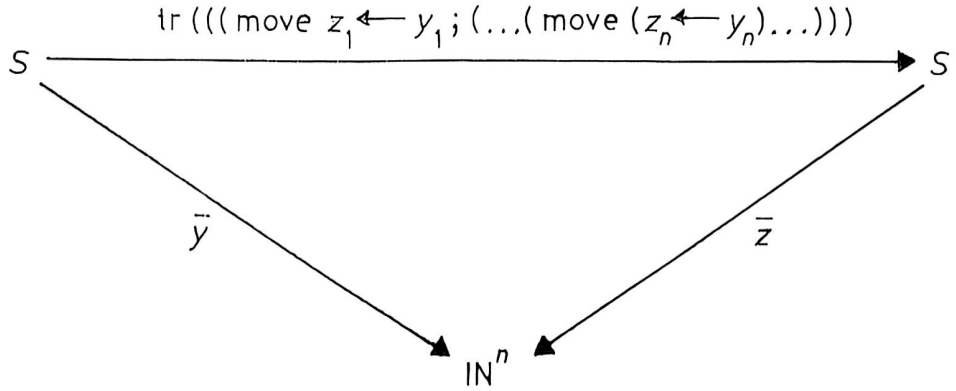
Demonstrație. Etapa I. Folosind lema 2, arătăm că mulțimea funcțiilor LOOP-calculabile conține funcțiile α, β, $1_{\mathbb{N}}$, s. Într-adevăr, funcția α este calculată de $[v, \wedge, \wedge]$, deci de programul $\wedge$ prin selecția $(v, \wedge)$, variabila $v \in V$ fiind arbitrară dar fixată. Funcția β este calculată de $[\wedge, \mathit{clear}\ v, v]$, deci de programul *clear* v prin selecția $(\wedge, v)$, $\forall\, v \in V$. De asemenea, $1_{\mathbb{N}}$ și s sînt calculate, respectiv, de $[v, \wedge, v]$ și $[v, \mathit{incr}\ v, v]$, $v \in V$ fiind arbitrar fixat.

Etapa a II-a. Arătăm că mulțimea funcțiilor LOOP-calculabile este închisă la compoziție, combinație și exponențiere.

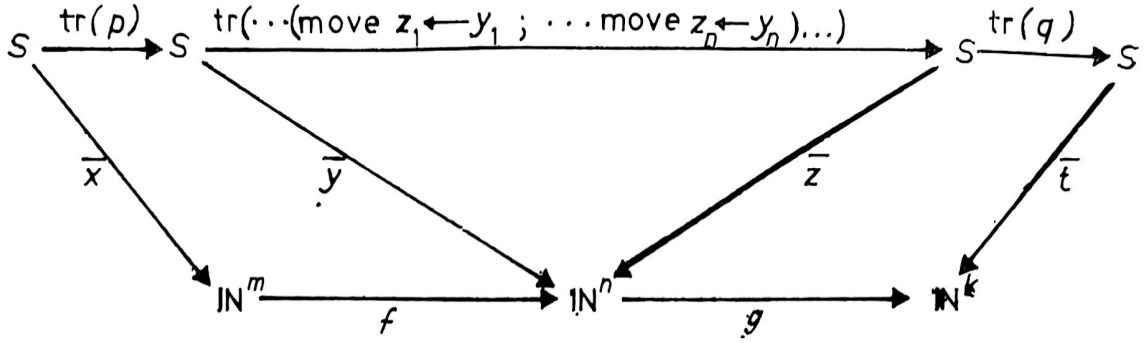
a) *Închiderea la compunere.* Fie $f : \mathbb{N}^m \to \mathbb{N}^n$, $g : \mathbb{N}^n \to \mathbb{N}^k$ funcţii LOOP-calculabile. Conform observaţiei care succede lema 1, putem presupune că

$$f = [\bar{x}, p, \bar{y}], \quad g = [\bar{z}, q, \bar{t}] \text{ şi } \bar{y} \cap \bar{z} = \emptyset.$$

Atunci $g \circ f = [\bar{x}, (p\,;((move\ z_1 \leftarrow y_1\,;\ (\ldots(move\ z_n \leftarrow y_n)\ldots))\,;q)), \bar{t}]$, adică $g \circ f$ este calculată de programul $p\,;\ move\ z_1 \leftarrow y_1\,;\ldots;\ move\ z_n \leftarrow y_n\,;\ q$ prin selecţia $(\bar{x}, \bar{t})$, $n \geqslant 1$. Într-adevăr, se arată prin inducţie după n că diagrama următoare este comutativă :

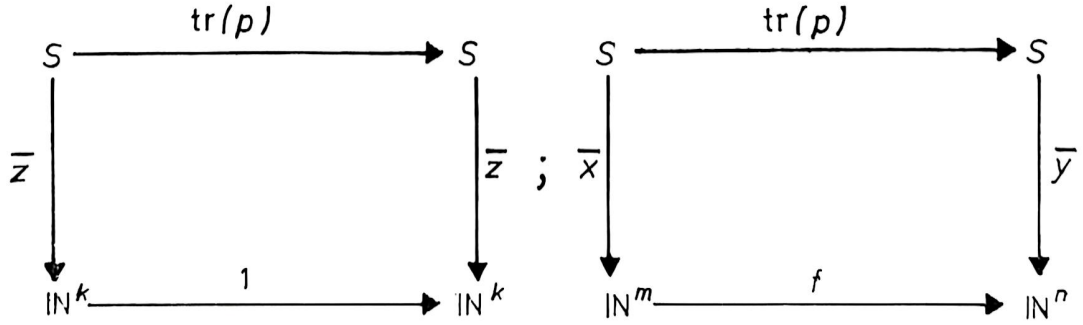


şi acelaşi lucru pentru diagrama :

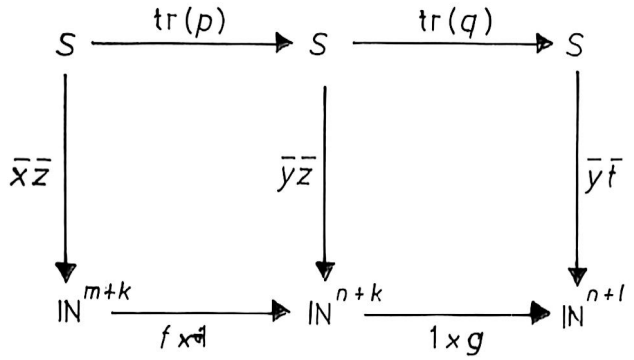


b) *Închiderea la combinaţie.* Fie $f : \mathbb{N}^m \to \mathbb{N}^n$, $g : \mathbb{N}^k \to \mathbb{N}^l$ LOOP-calculabile. Conform afirmaţiei care succede lema 1, putem presupune că $f = [\bar{x}, p, \bar{y}]$, $g = [\bar{z}, q, \bar{t}]$ astfel încît $(\bar{z} \cup \mathrm{var}\,(q) \cup \bar{t}) \cap \cap\, (\bar{x} \cup \mathrm{var}\,(p) \cup \bar{y}) = \emptyset$. Atunci combinaţia $f \times g : \mathbb{N}^{m+k} \to \mathbb{N}^{n+l}$, $(u, v) \mapsto (f(u), g(v))$ este tocmai $f \times g = [\bar{x}\bar{z}, (p\,;q), \bar{y}\bar{t}]$.

Conform proprietăţii 3) de la p. 154 şi ipotezei, diagramele de mai jos sînt comutative, $\bar{y}\bar{z} \circ \mathrm{tr}\,(p) = (f \times 1)(\bar{x}\,\bar{z})$. Apoi, $\bar{y} \circ \mathrm{tr}\,(q) =$



$= 1_{\mathbb{N}^n} \circ \bar{y}$, deci $\bar{y}\,\bar{t} \circ \mathrm{tr}\,(q) = (1_{\mathbb{N}^n} \times g) \circ \bar{y}\bar{z}$. De aici rezultă diagrama comutativă :



Deoarece $(f \times 1) \circ (1 \times g) = f \times g$, se obţine $\bar{y}\bar{t} \circ \mathrm{tr}\,((p\,;q))$ $(f \times g)(\bar{x}\,\bar{z})$ şi ca atare $f \times g$ este LOOP-calculabilă.

c) *Închiderea la exponenţiere.* Fie $f : \mathbb{N}^n \to \mathbb{N}^n$ o funcţie LOOP-calculabilă şi $f = [\bar{x}, p, \bar{y}]$. Fie $v \notin \bar{x} \cup \mathrm{var}\,(p) \cup \bar{y}$. Atunci pentru funcţia $f^{\#} : \mathbb{N}^{n+1} \to \mathbb{N}^n$, $f^{\#}(\bar{x}, y) = f^y(\bar{x})$, avem $f^{\#} = [\bar{x}v,$ *loop* v : $:(p\,;(\ldots(move\ x_1 \leftarrow y_1\,;\ldots\,;\ move\ x_n \leftarrow y_n)\ldots),\ end, \bar{y}]$, adică $f^{\#}$ este calculată de programul *loop* $v : p\,;\ move\ x_1 \leftarrow y_1\,;\ldots\,;\ move\ x_n \leftarrow y_n$ *end*, prin selecţia $(\bar{x}v, \bar{y})$.

E t a p a a III-a. Arătăm că orice funcţie LOOP-calculabilă este primitiv recursivă. Începem cu o lemă simplă, care se demonstrează prin inducţie pe programe.

LEMA 3. $\forall\, p \in P$, *selecţia* $(\overline{\mathrm{var}\,(p)}, \overline{\mathrm{var}\,(p)})$ *este funcţională pentru* p, *iar* $[\overline{\mathrm{var}\,(p)},\ p,\ \overline{\mathrm{var}\,(p)}]$ *este primitiv recursivă.*

Fie acum $f = [\bar{x}, p, \bar{y}]$ o funcţie LOOP-calculabilă. Putem pune $\bar{x} = \bar{x}_1\bar{x}_2$ unde $\bar{x}_1 \cap \mathrm{var}\,(p) = \emptyset$, $\bar{x}_2 \subset \mathrm{var}\,(p)$, compunînd eventual cu o funcţie de rearanjare. În mod similar, $\bar{y} = \bar{y}_1\bar{y}_2$, unde $\bar{y}_1 \cap \mathrm{var}\,(p) = \emptyset$, $\bar{y}_2 \subset \mathrm{var}\,(q)$.

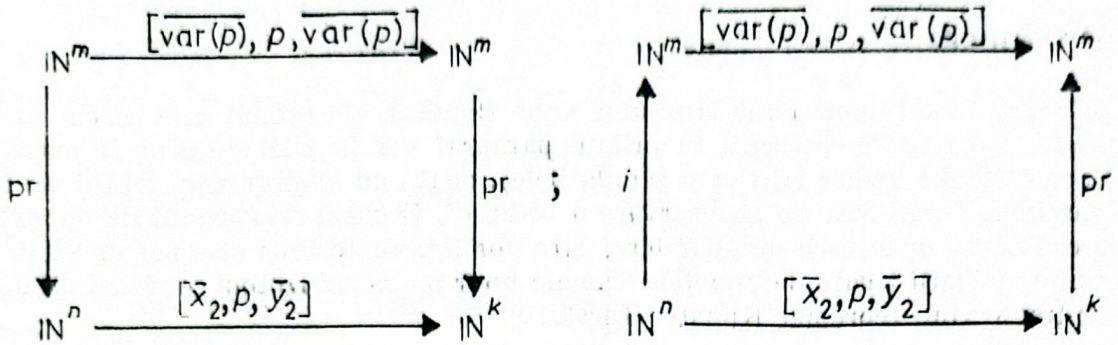
Arătăm că $\bar{y}_1 \subset \bar{x}_1$ [altminteri putem găsi s, s' care coincid pe $\bar{x}$ dar nu coincid pe $\bar{y}_1$. Conform proprietăţii 3 de la p. 154, $\mathrm{tr}\,(p)(s)$ şi, respectiv, $\mathrm{tr}(p)(s')$ coincide cu s, respectiv cu s' pe $V \setminus \mathrm{var}\,(p)$, deci $\mathrm{tr}(p)(s)$ şi $\mathrm{tr}(p)(s')$ nu coincid pe $\bar{y}_1$ şi nici pe $\bar{y}$, ceea ce contrazice funcţionalitatea selecţiei $(\bar{x}, \bar{y})$]. Aşadar, $(\bar{x}_1, \bar{y}_1)$ este funcţională pentru p şi $f_1 = [\bar{x}_1, p, \bar{y}_1]$ este primitiv recursivă, deoarece este o proiecţie, conform proprietăţii 3 amintite.

Arătăm acum că selecţia $(\bar{x}_2, \bar{y}_2)$ este funcţională pentru p. [Dacă nu ar fi astfel, atunci ar exista s, s' astfel încît $\bar{x}_2(s) = \bar{x}_2(s')$ şi $\bar{y}_2(\mathrm{tr}\,(p)(s)) \neq \bar{y}_2(\mathrm{tr}\,(p)(s'))$. Fie

$$s'' = \begin{cases} s' & \text{pe } V \setminus \bar{x}_1, \\ s & \text{pe } \bar{x}_1, \end{cases}$$

deci $\overline{x}(s) = \overline{x}(s'')$. Dar selecția $(\overline{\text{var}(p)}, \overline{\text{var}(p)})$ este funcțională pentru p, conform lemei 3. Deoarece $\overline{\text{var}(p)}(s') = \overline{\text{var}(p)}(s'')$, rezultă $\overline{\text{var}(p)}(\text{tr}(p)(s')) = \overline{\text{var}(p)}(\text{tr}(p)(s''))$, deci $\overline{y}_2(\text{tr}(p)(s')) = \overline{y}_2(\text{tr}(p)(s'')) = \overline{y}_2(\text{tr}(p)(s)) \neq \overline{y}_2(\text{tr}(p)(s''))$ și prin urmare $\overline{y}(\text{tr}(p)(s)) \neq \overline{y}(\text{tr}(p)(s''))$, ceea ce contrazice funcționalitatea selecției $(\overline{x}, \overline{y})$.]

Arătăm în fine că $f_2 = [\overline{x}_2, p, \overline{y}_2]$ este primitiv recursivă; într-adevăr, dacă $\overline{\text{var}(p)}$ are m elemente $(m \geqslant n, m \geqslant k)$, atunci diagramele sînt comutative, unde $i = 1_{\mathbb{N}^n} \times \overbrace{\beta \times \ldots \times \beta}^{m-n}$ și „pr" reprezintă



proiecții canonice. Deoarece i și pr sînt funcții primitiv recursive, rezultă că f_2 este primitiv recursivă. În concluzie, $[\overline{x}, p, \overline{y}] = f_1 \times f_2$ este primitiv recursivă. Teorema 3.5 este complet demonstrată. ∎

CAPITOLUL 4

ORDINE, DINAMICĂ DISCRETĂ ȘI PROGRAMARE RAȚIONALĂ

Introducere

Acest capitol este consacrat studiului unor structuri de ordine care joacă un rol important în matematica discretă. În primul paragraf vor fi prezentate unele clase de mulțimi ordonate (incluzînd laticile și semilaticile), odată cu analiza proprietății de izotonie, care modelează ideea de „conservare a ordinii". O clasă importantă de operatori izotoni o constituie operatorii de închidere, care vor fi caracterizați complet în § 4.2. Se cunosc multe aplicații legate de punctele fixe ale unor operatori izotoni convenabili, unde un rol central revine teoremei Knäster-Tarski.

Conceptul de monoid complet ordonat introdus în ([48], [12], [7]) este important și pentru sine, dar totodată el permite o extindere sensibilă a teoremei lui Kleene asupra limbajelor. Acest cerc de idei este prezent în ultima parte a capitolului, odată cu cîteva aplicații în programare.

§ 4.1. LATICI COMPLETE, SISTEME DE ÎNCHIDERE

Reamintim că o mulțime ordonată (pe scurt m.o.) este o mulțime pe care este fixată o relație de ordine parțială. Dacă $(M, \leqslant)$ este o m.o., atunci $\forall x \in M,\ x \leqslant x$; $\forall\ x,y,z \in M,\ x \leqslant y, y \leqslant z \Rightarrow x \leqslant z$; $\forall\ x,y \in M,\ x \leqslant y, y \leqslant x \Rightarrow x = y$. Se poate considera un graf în care vîrfurile sînt elementele lui M și două vîrfuri x, y sînt unite printr-un arc dacă și numai dacă $x < y$ și nu există $z \in M$ astfel încît $x \leqslant z$, $z \leqslant y$. În figura 4.1 sînt indicate grafurile pentru $M = \mathbb{N}$ cu ordinea $\leqslant$ uzuală și pentru $M = \mathbf{p}(\mathbb{B})$ cu ordinea dată de incluziune. Reamintim de asemenea că dacă $(M, \leqslant)$ și $(N, \subseteq)$ sînt două mulțimi

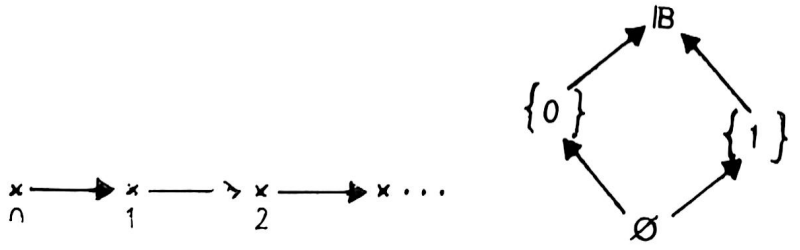


Fig. 4.1

ordonate, atunci o aplicație $f : M \to N$ se numește izotonă dacă $\forall\, x, y \in M,\ x \leqslant y \Rightarrow f(x) \subseteq f(y)$.

Z-părți ale unei m.o.

DEFINIȚIA 4.1. Presupunem că oricărei m.o. M i se asociază o colecție de părți Z_M ale lui M ($Z_M \subset \mathbf{p}(M)$) astfel încît să fie verificate condițiile următoare:

1) $\forall\, x_0, x_1 \in M,\ x_0 \leqslant x_1 \Rightarrow \{x_0, x_1\} \in Z_M$; în particular, $\forall\, x \in M$, $\{x\} \in Z_M$;

2) pentru orice aplicație izotonă $f : M \to N$ și $\forall\, S \in Z_M$, să avem $f(S) \in Z_N$.

Se spune atunci că este definit un *sistem de părți* Z iar elementele lui Z_M se numesc *Z-părți ale lui M*, oricare ar fi m.o. M. Dacă Z' este un alt sistem de părți și dacă pentru orice m.o. avem $Z_M \subset Z'_M$, atunci se scrie $Z \subset Z'$.

Exemple. 1) Vom nota prin **2** sistemul de părți de forma $\{x_0, x_1\}$, cu $x_0 \leqslant x_1$. Se notează p sistemul de părți definit luînd $\mathbf{p}_M = \mathbf{p}(M)$ pentru orice m.o. M. Pentru orice sistem de părți Z avem evident $\mathbf{2} \subset Z \subset \mathbf{p}$.

2) Se notează cu f sistemul părților finite definite prin $\mathbf{f}_M = \{A \subset M \mid A \text{ finită}\}$, pentru orice m.o. M.

3) O submulțime $D \subset M$ a unei m.o. M se numește *dirijată* dacă pentru orice parte finită F a lui D, D conține un majorant pentru F (în particular, luînd $F = \emptyset$ rezultă că D este nevidă). Părțile dirijate ale mulțimilor ordonate formează un sistem de părți notat Δ. Se poate de asemenea considera sistemul **l** al lanțurilor (adică al părților liniar ordonate nevide); evident, $\mathbf{l} \subset \Delta$.

4) Numim *ω-parte* a unei m.o. M orice submulțime $A \subset M$ care admite o numărare (în sensul definit în § 2.3) și în plus este izotonă; așadar, există o funcție izotonă surjectivă $g : \mathbb{N} \to A$. Dacă $x_0 \leqslant x_1$, atunci definim $g(0) = x_0$ și $g(n) = x_1$ pentru $n \geqslant 1$, deci $\{x_0, x_1\}$ este o ω-parte. Apoi, dacă o aplicație $f : M \to N$ este izotonă, $S \subset M$ este o ω-parte și $g : \mathbb{N} \to S$ este izotonă și surjectivă, atunci aplicația $(f|S) \circ g : \mathbb{N} \to f(S)$ este izotonă și surjectivă, deci $f(S)$ este o ω-parte a lui $\mathbb{N}$. Se obține astfel un sistem de părți, notat ω.

M.o. Z-complete. Latici complete

DEFINIȚIA 4.2. Fiind dat un sistem de părți Z, o m.o. M se numește *Z-completă* dacă orice Z-parte $A \subset M$ are margine superioară (adică $\forall\, A \in Z_M,\ \exists \sup A$).

Dacă M este Z-completă și dacă $\emptyset, M \in Z_M$, atunci vom folosi sistematic următoarele notații:

$\bot = \sup \emptyset$ (= cel mai mic element al lui M);

$\top = \sup M$ (= cel mai mare element al lui M).

Mulțimile ordonate **p**-complete se numesc *latici complete* iar cele **f**-complete se numesc *semilatici* (avînd cel mai mic element).

Exemple. 1) Orice m.o. este **2**-completă. Apoi, dacă $Z \subset Z'$, atunci orice mulțime Z' este Z-completă.

2) Pentru orice mulțime X, $(\mathbf{p}(X), \subset)$ este o latice completă, iar mulțimea părților finite ale lui X, ordonată prin incluziune, este o semilatice.

3) Fie (Ω, ν) o signatură și X o Ω-algebră fixată (definiția 3.9); vom identifica tacit simbolurile de operații cu operațiile însele. Definim acum un concept dual celui de subalgebră. Se numește *congruență pe* X orice relație de echivalență ρ pe X compatibilă cu operațiile din Ω; așadar, $\rho \subset X^2$ și $\forall \omega \in \Omega$, $\nu(\omega) = n$, din faptul că $x_1 \rho y_1, \ldots, x_n \rho y_n$, rezultă că $\omega(x_1, \ldots, x_n)\ \rho\omega(y_1, \ldots, y_n)$.

Notăm cu $S(X)$ colecția tuturor subalgebrelor lui X (ordonată prin incluziune) și cu $C(X)$ colecția tuturor congruențelor pe X (de asemenea ordonată prin incluziune: $\rho_1 \leqslant \rho_2 \leftrightarrow \rho_1 \subset \rho_2$). Dacă $X_1, X_2 \in S(X)$ sînt două subalgebre ale lui X, atunci se pot considera intersecția $X_1 \cap X_2 = X_1 \wedge X_2$ și suma $X_1 + X_2 = X_1 \wedge X_2$ (subalgebra lui generată X de reuniunea $X_1 \cup X_2$). Pe de altă parte, dacă $\rho_1, \rho_2 \in C(X)$, notăm cu $\rho_1 \cap \rho_2 \in C(X)$ intersecția și cu $\rho_1 \vee \rho_2 = \inf \{\rho \in C(X) \mid \rho_1 \leqslant \rho,\ \rho_2 \leqslant \rho\} \in C(X)$. Se arată ușor că $S(X)$ formează o latice completă (*laticea subalgebrelor* lui X) și de asemenea $C(X)$ este o latice completă (*laticea congruențelor pe* X).

TEOREMA 4.1. *O mulțime ordonată* $(M, \leqslant)$ *este o latice completă dacă și numai dacă orice submulțime* $A \subset M$ *admite* $\inf A$.

Demonstrație. Fie M o latice completă, adică orice parte a lui M admite margine superioară. Arătăm că o parte $A \subset M$, oarecare, admite și margine inferioară. Pentru aceasta, să notăm cu B mulțimea minoranților lui A. Atunci $\forall\, a \in A$, $b \leqslant a$, pentru orice $b \in B$. Deci $\sup B \leqslant a$. Atunci $\sup B \in B$ și ca atare există $\inf A$ și $\inf A = \sup B$. Afirmația inversă se demonstrează similar. ∎

Reținem că *o latice completă* $(L, \leqslant)$ *este o m.o. în care orice parte are margine inferioară și margine superioară*; în particular, există $\bot$ și $\top$ în L.

Orice latice completă este evident o latice și o semilatice.

Aplicații Z-continue

DEFINIȚIA 4.3. Fie Z un sistem de părți și M, N două m.o. Z-complete. O aplicație $f: M \to N$ se numește *Z-continuă* dacă $\forall\, A \in Z_M$, $f(\sup A) = \sup f(A)$. Aplicațiile **p**-continue se numesc pe scurt *continue*.

Exemple. 1) Evident, o aplicație $f: M \to N$ este 2-continuă dacă și numai dacă f este izotonă, iar dacă $Z \subset Z'$ și f este Z'-continuă, atunci f este Z-continuă.

2) Fie Ω o signatură și $h: X \to Y$ un morfism de Ω-algebre. Pentru orice congruență σ pe Y se poate defini o congruență pe X, notată $h \circ \sigma$: $\forall\, x_1, x_2 \in X$, $x_1 (h \circ \sigma) x_2 \leftrightarrow h(x_1)\ \sigma\ h(x_2)$.

Se pot considera patru aplicații remarcabile:

$$h_s : S(X) \to S(Y), \quad X_1 \mapsto h(X_1) = \{h(x) \mid x \in X_1\};$$

$$h_c : C(Y) \to C(X), \quad \sigma \mapsto h \circ \sigma = (h \times h)^{-1}(\sigma);$$

$$h_s^{-1} : S(Y) \to S(X), \quad Y_1 \mapsto h^{-1}(Y_1) = \sup \{X_1 \mid h(X_1) \subset Y_1\};$$

$$h_c^{-1} : C(X) \to C(Y), \quad \rho \mapsto \inf \{\sigma \in C(Y) \mid \rho \leqslant h_c(\sigma)\}.$$

Se verifică ușor că $\forall\, X_1, X_2 \in S(X)$, $h_s(X_1 \vee X_2) = h_s(X_1) \vee h_s(X_2)$ și că $\forall\, \sigma_1, \sigma_2 \in C(Y)$, $h_c(\sigma_1 \wedge \sigma_2) = h_c(\sigma_1) \wedge h_c(\sigma_2)$ și, mai general, $\forall\, \mathcal{S} \subset S(X)$, $h_s(\sup \mathcal{S}) = \sup_{X_1 \in \mathcal{S}} h_s(X_1)$ și $\forall\, \mathcal{C} \subset C(Y)$, $h_c(\inf \mathcal{C}) = \inf_{\sigma \in \mathcal{C}} h_c(\sigma)$; în particular, h_s este 1-continuă.

De asemenea, h_s^{-1} conservă inf și h_c^{-1} conservă sup. În fine, observăm că aplicația $h_s^{-1} \circ h_s : S(X) \to S(X)$ este l-continuă.

TEOREMA 4.2. *Fie Z un sistem de părți. O aplicație $f : M \to N$ între două m.o. Z-complete este izotonă* $\leftrightarrow \forall A \in Z_M$, $\sup f(A) \leqslant f(\sup A)$.

În particular, orice aplicație Z-continuă este izotonă.

Demonstrație. Dacă f este izotonă, atunci $\forall x \in A$, avem $x \leqslant \sup A$ și $f(x) \leqslant f(\sup A)$. Deoarece $f(x) \in f(A)$, rezultă că $\sup f(A) \leqslant f(\sup A)$. Reciproc, fie $\forall x_0 \leqslant x_1$ în M, deci $B = \{x_0, x_1\} \in Z_M$. Atunci

$$f(x_1) = f(\sup B) \geqslant \sup f(B) = \sup \{f(x_0), f(x_1)\} \geqslant f(x_0),$$

deci f este izotonă. ∎

COROLAR (*continuitatea luării supremumului*). *Fie Z un sistem de părți și M o m.o. Z-completă. Presupunem că $Z_M \subset \mathbf{p}(M)$ este Z-completă relativ la incluziune. Atunci aplicația*

$$\sup : Z_M \to M, \quad A \mapsto \sup A$$

este Z-continuă.

Demonstrație. Dacă $A \subset B$ sînt mulțimi din Z_M, atunci $\sup A \leqslant \sup B$, deci funcția „sup" este izotonă și, conform teoremei 4.2, rezultă că pentru orice familie $\{A_i\}_{i \in I}$ de Z-părți ale lui M, avem

$$\sup \left(\bigcup_{i \in I} A_i\right) \geqslant \sup_{i \in I} (\sup A_i).$$

Rămîne de dovedit inegalitatea contrară. Este suficient de observat că $\forall x \in \bigcup_{i \in I} A_i$, $\exists j \in I$ astfel ca $x \in A_j$ și prin urmare $x \leqslant \sup A_j \leqslant \sup_{i \in I} (\sup A_i)$. ∎

Observație. Corolarul anterior se aplică pentru $Z = \mathbf{2}, \mathbf{f}, \mathbf{p}, \mathbf{l}, \Delta$. Aplicînd tocmai acest corolar pentru $\mathbf{p}$, este permisă, de exemplu, înlocuirea lui $\sup_{x \in \bigcup_{i \in I} X_i}$ cu $\sup_{i \in I} \sup_{x \in X_i}$ și a lui $\sup_{x \in X} \sup_{y \in Y}$ cu $\sup_{y \in Y} \sup_{x \in X}$.

O definiție echivalentă a semilaticilor

Reamintim că o semilatice $(S, \leqslant)$ este o mulțime ordonată $\mathbf{f}$-completă, deci orice parte finită a lui S admite margine superioară. Punînd $\perp = \sup \emptyset$ și $\forall a, b \in S$, $a \vee b = \sup \{a, b\}$, rezultă imediat că $\forall a, b, c \in S$ au loc proprietățile următoare:

1) $a \vee (b \vee c) = (a \vee b) \vee c$;

2) $\perp \vee a = a \vee \perp = a$;

3) $a \vee b = b \vee a$;

4) $a \vee a = a$;

5) $a \leqslant b \leftrightarrow a \vee b = b$.

Atunci $(S, \vee, \perp)$ este un monoid comutativ în care toate elementele sînt idempotente ($\forall\, x \in S,\ x^2 = x$). Invers, dacă $(S, \vee, \perp)$ este un astfel de monoid, atunci se definește o relație de ordine „$\leqslant$" pe S punînd $a \leqslant b \leftrightarrow a \vee b = b$, iar $(S, \leqslant)$ este o semilatice în care $\forall\, a, b \in L$, $\sup\{a, b\} = a \vee b$ și $\sup \emptyset = \perp$. Reținem că *o m.o.* $(S, \leqslant)$ *este o semilatice dacă și numai dacă* $\forall\, a, b \in S$, *există* $\sup\{a, b\} = a \vee b$ *și* S *are un cel mai mic element.*

În plus, se verifică ușor că dacă $(S, \leqslant)$ și $(S', \leqslant)$ sînt două semilatici și $g : S \to S'$ este o aplicație, atunci:

— g este izotonă $\leftrightarrow \forall\, a, b \in S,\ g(a) \vee g(b) \leqslant g(a \vee b)$;

— g este f-continuă $\leftrightarrow \forall\, a, b \in S,\ g(a \vee b) = g(a) \vee g(b)$ și $g(\perp) = \perp$.

O definiție echivalentă a laticilor complete

Conform corolarului teoremei 4.2, pentru orice latice completă $(L, \leqslant)$, funcția $\sigma : \mathbf{p}(L) \to L$, $A \mapsto \sup A$ este continuă, adică pentru orice familie $\{A_i\}_{i \in I}$ de părți $A_i \subset L$ avem $\sigma(\bigcup_{i \in I} A_i) = \sup_{i \in I} (\sup A_i)$.

Fiind dată o mulțime nevidă L, să presupunem că există o funcție $\sigma : \mathbf{p}(L) \to L$ cu proprietatea că pentru orice familie $\{A_i\}_{i \in I}$ de părți $A_i \subset L$, avem $\sigma(\bigcup_{i \in I} A_i) = \sigma(\{\sigma(A_i) \mid i \in I\})$. Pentru orice $x, y \in L$ să punem $x \vee y = \sigma(\{x, y\})$. Atunci pe L se obține o relație de ordine punînd $x \leqslant y \leftrightarrow x \vee y = y$ și, în plus, pentru orice $A \subset L$ există $\sup A$, egal cu $\sigma(A)$, deci L este o latice completă.

Observație. Fie X o mulțime oarecare. Atunci $\mathbf{p}(X)$ este evident o latice completă (relativ la incluziune). Are loc următoarea *proprietate de universalitate a lui* $\mathbf{p}(X)$: *pentru orice latice completă* L *și oricare ar fi o funcție* $f : X \to L$, *există și este unică o aplicație continuă* $\bar{f} : \mathbf{p}(X) \to L$ *astfel încît* $\forall\, x \in X,\ \bar{f}(\{x\}) = f(x)$.

[Într-adevăr, pentru orice $A \subset X$ să punem $\bar{f}(A) = \sup f(A)$. Atunci $\bar{f}(\bigcup_{i \in I} A_i) = \sup f(\bigcup_{i \in I} A_i) = \sup \bigcup_{i \in I} f(A_i) = \sup_{i \in I} \sup f(A_i) = \sup_{i \in I} \bar{f}(A_i)$, utilizînd continuitatea lui „sup". Așadar, $\bar{f}$ este continuă. Apoi, $\forall\, x \in X$, $\bar{f}(\{x\}) = \sup \bar{f}(\{x\}) = \sup f\{(x)\} = f(x)$. Rămîne de dovedit unicitatea lui $\bar{f}$; pentru aceasta să observm că oricare ar fi funcția $g : \mathbf{p}(X) \to L$ continuă și astfel încît $g(\{x\}) = f(x)$, $\forall\, x \in X$, avem pentru orice $A \subset X$, $g(A) = g(\bigcup_{x \in A} \{x\}) = \sup_{x \in A} g(\{x\}) = \sup_{x \in A} f(x) = \sup f(A) = \bar{f}(A)$.]

Dacă se notează cu $\mathbf{C}_p$ categoria laticilor complete și aplicațiilor continue, dacă se consideră functorul ștergător $U : \mathbf{C}_p \to \mathbf{Set}$, aplicația $G : \mathrm{Ob}\,\mathbf{Set} \to \mathrm{Ob}\,\mathbf{C}_p$, $X \mapsto \mathbf{p}(X)$ și dacă pentru orice mulțime X se definește aplicația $I_X : X \to U(G(X))$, $x \mapsto \{x\}$, atunci proprietatea de universalitate anterioară, împreună cu definiția 3.7, arată că U are adjunct și că pentru orice mulțime X, $\mathbf{p}(X)$ este un $\mathbf{C}_p$-obiect liber generat de X (numit *laticea completă generată de* X).

În mod similar se arată că pentru orice mulțime X, $\mathfrak{f}(X) = \{F \subset X \mid F \text{ finită}\}$ este o semilatice relativ la incluziune și că pentru orice semilatice S, oricare ar fi o funcție $g : X \to S$, există și este unică o funcție f-continuă $\bar{g} : \mathfrak{f}(X) \to S$ astfel încît $\forall\, x \in X$, $\bar{g}(\{x\}) = g(x)$. Cu alte cuvinte, $\mathfrak{f}(X)$ este semilaticea generată de X.

Părți inf-complete

Fie L o latice completă. O parte $C \subset L$ se numește *inf-completă* dacă pentru orice $A \subset C$, avem $\inf A \in C$. În acest caz, pentru orice $A \subset C$, există $\inf_C A$ (pentru ordinea indusă de pe L pe C) și coincide cu $\inf_L A$. Conform teoremei 4.1 mulțimea C cu ordinea indusă este și ea o latice completă. Cel mai mare element al lui C este $\top = \inf \emptyset \in C$, dar deși $\sup_C A$ există, el diferă în general de $\sup_L A$ (cu excepția cazului cînd $\sup_L A \in C$). Duala noțiunii de parte inf-completă este cea de parte **p**-completă (numită și sup-completă).

DEFINIȚIA 4.4. O parte a unei latici complete care este simultan inf-completă și sup-completă se numește *sublatice*. În cazul cînd $L = \mathfrak{p}(E)$, E fiind o mulțime oarecare (din universul $\mathcal{U}$), părțile inf-complete se numesc *sisteme de închidere pe* E. Așadar, o colecție $\mathcal{S}$ de părți ale lui E este un sistem de închidere dacă și numai dacă $E \in \mathcal{S}$ și intersecția oricărei familii de mulțimi din $\mathcal{S}$ este o mulțime din $\mathcal{S}$. În mod dual, se numește *sistem de deschidere* pe E orice colecție $\mathcal{T}$ de părți ale lui E astfel încît $\emptyset \in \mathcal{T}$ și reuniunea oricărei familii de părți din $\mathcal{T}$ aparține lui $\mathcal{T}$.

Exemple. 1) Dacă $Z \subset Z'$, atunci părțile Z-complete ale unei m.o. Z'-complete formează un sistem de închidere.

2) O *topologie* pe o mulțime E este un sistem de deschidere $\mathcal{T} \subset \mathfrak{p}(E)$ în care intersecția oricărei familii finite de părți din $\mathcal{T}$ este tot în $\mathcal{T}$ (în particular, $E \in \mathcal{T}$ ca intersecție a familiei vide). Sublaticile lui $\mathfrak{p}(E)$ se mai numesc *supratopologii*. Asupra supratopologiilor vom reveni ulterior.

Operatori de închidere

Noțiunea de operator de închidere este esențialmente echivalentă cu cea de parte inf-completă, dar este utilă și prin ea însăși.

DEFINIȚIA 4.5. Fie $(L, \leqslant)$ o latice completă (deci o m.o. în care pentru orice parte $C \subset L$ există $\inf C$ și $\sup C$). Se numește *operator izoton al lui* L orice aplicație izotonă

$$c : L \to L.$$

Un operator izoton $c : L \to L$ se numește **operator de închidere** dacă este *extensiv* (adică $\forall\, x \in L$, $x \leqslant c(x)$) și *idempotent* (adică $c^2 = c$, deci $\forall\, x \in L$, $c(c(x)) = c(x)$).

Pentru $C \subset L$ și $x \in L$ vom nota

$$C_x = \{y \in C \mid x \leqslant y\}.$$

Lema următoare exprimă esența legăturii între operatorii de închidere și părțile inf-complete.

LEMA 1. *Fie L o latice completă.*

a) *Dacă $c : L \to L$ este un operator de închidere, atunci are loc relația $c(L) = \{x \in L \mid c(x) = x\}$ și, în plus, $c(L)$ este o parte inf-completă a lui L.*

b) *Dacă $C \subset L$ este o parte inf-completă a lui L, atunci $\forall\, x \in L$, $\inf C_x \in C_x$ (deci C_x are un cel mai mic element).*

c) *Fie $C \subset L$ o submulțime astfel încît $\forall\, x \in L$, $\inf C_x \in C_x$; atunci aplicația $c : L \to L$, $x \mapsto \inf C_x$ este un operator de închidere și $c(L) = C$.*

d) *Dacă $c : L \to L$ este un operator de închidere și notăm $C = c(L)$, atunci $\forall\, x \in L$, $c(x) = \inf C_x$.*

e) *O parte $C \subset L$ este inf-completă dacă și numai dacă $\forall\, x \in L$, C_x admite un cel mai mic element;*

f) *Dacă $c_1, c_2 : L \to L$ sînt operatori izotoni, extensivi și idempotenți, astfel încît $c_1(L) = c_2(L)$, atunci $c_1 = c_2$.*

Demonstrație. a) Dacă $x = c(x)$, atunci $x \in c(L)$; apoi, pentru $x \in c(L)$, $x = c(y)$, deci $c(x) = c(c(y)) = c^2(y) = c(y) = x$. Apoi, fie $A \subset c(L)$; evident, $\inf A \leqslant c(\inf A)$, folosind extensivitatea lui c. Dar $\forall\, a \in A$, $\inf A \leqslant a$, deci $c(\inf A) \leqslant c(a) = a$ și prin urmare $c(\inf A) \leqslant \inf A$, adică $\inf A \in c(L)$.

b) Avem $\inf C_x \in C$ și, evident, $\inf C_x \geqslant x$.

c) Arătăm mai întîi că operatorul c este izoton : dacă $x \leqslant y$ în L, atunci $C_x \supset C_y$, deci $\inf C_x \leqslant \inf C_y$, adică $c(x) \leqslant c(y)$; apoi, $\forall\, y \in C_x$, $x \leqslant y$, de unde $x \leqslant \inf C_x = c(x)$, deci c este extensiv. De asemenea, să observăm că $\forall\, x \in L$, $c(x) = \inf C_x \in C_x \subset C$, deci $c(x) \in C_{c(x)}$ și prin urmare $c(c(x)) = \inf C_{c(x)} \leqslant c(x)$. Deoarece c este extensiv și izoton, rezultă $c(x) \leqslant c(c(x))$, deci $c(x) = c(c(x))$, adică $c = c^2$. În fine, are loc relația $c(L) = C$ [într-adevăr, $\forall\, x \in L$, $c(x) \in C$, deci $c(L) \subset C$ iar dacă $x \in C$, atunci $x \in C_x$, deci $\inf C_x = x$ și ca atare $x = c(x) \in c(L)$].

d) Deoarece $c(x) \in C$ și $x \leqslant c(x)$, rezultă $c(x) \in C_x$, pentru orice $x \in L$. Dacă $y \in C_x$, atunci $x \leqslant y$, deci $c(x) \leqslant c(y) = y$, deoarece $y \in c(L)$. Așadar, $c(x)$ este cel mai mic element al lui C_x și, în particular, coincide cu $\inf C_x$.

e) O implicație rezultă direct din b), iar cealaltă rezultă din punctele c) și a).

f) Fie $\forall\, x \in L$; atunci $x \leqslant c_1(x)$. Dar există $y \in L$ astfel încît $c_1(x) = c_2(y)$, deci $x \leqslant c_2(y)$ și, cum c_2 este izoton și idempotent, $c_2(x) \leqslant c_2(y)$, adică $c_2(x) \leqslant c_1(x)$. În mod similar, $c_1(x) \leqslant c_2(x)$, deci $c_1(x) = c_2(x)$. ∎

TEOREMA 4.3. *Pentru orice latice completă există o corespondență bijectivă între mulțimea părților inf-complete și mulțimea operatorilor de închidere.*

Demonstrație. Fie L o latice completă. Conform lemei 1, a), oricărui operator de închidere $c : L \to L$ îi putem asocia partea inf-completă $c(L)$. Conform punctelor b), c) ale lemei 1, oricărei părți inf-complete $C \subset L$ îi putem asocia operatorul de închidere $c : L \to L$, $x \mapsto \inf C_x$. Tot din lema 1 (pct. c) și d)) rezultă că aceste două asocieri sînt aplicații inverse una alteia. ∎

În cele ce urmează, prin operator de închidere asociat unei părți inf-complete și prin parte inf-completă asociată unui operator de închidere vom înțelege construcțiile descrise mai sus.

În mod dual se poate defini noțiunea de operator de deschidere al unei latici complete L ca fiind o aplicație $o : L \to L$ izotonă, restrictivă ($\forall\, x \in L$, $o(x) \leqslant x$) și idempotentă. Teorema 4.3 se poate atunci dualiza și se obține o corespondență bijectivă între părțile sup-complete ale lui L și operatorii de deschidere.

COROLAR 1. *Fie L o latice completă, $C \subset L$ o parte inf-completă și $c : L \to L$ operatorul de închidere asociat. Atunci*

a) *pentru orice $A \subset C$, avem*

$$\sup_C A = c(\sup_L A);$$

b) *aplicația de corestricție $c : L \to c(L)$ este continuă.*

Demonstrație. a) Într-adevăr, avem $\sup_L A \leqslant c(\sup_L A)$, deci $c(\sup_L A)$ este un majorant pentru A și aparține lui $c(L) = C$. Dacă $x \in C$ este un alt majorant al lui A, atunci $\sup_L A \leqslant x$, deci $c(\sup_L A) \leqslant c(x) = x$.

b) Avem deci de arătat că $\forall\, A \subset L$, $\sup_C c(A) = c(\sup_L c(A))$. Pentru aceasta, să observăm mai întîi că $\forall\, a \in A$, $a \leqslant c(a) \leqslant \sup_L c(A)$, deci $\sup_L A \leqslant \sup_L c(A)$ și $c(\sup_L A) \leqslant c(\sup_L c(A))$. Apoi, $\forall\, a \in A$, $a \leqslant \sup_L A$, deci $c(a) \leqslant c(\sup_L A)$ și $\sup_L c(A) \leqslant c(\sup_L A)$, de unde $c(\sup_L c(A)) \leqslant c(c(\sup_L A)) = c(\sup_L A)$. ∎

Dacă asupra unui operator de închidere se pune în plus condiția de Z-continuitate (Z fiind un sistem de părți), ce se poate spune despre partea inf-completă asociată? Un răspuns este dat în

COROLAR 2. *Fie Z un sistem de părți, L o latice completă, $C \subset L$ o parte inf-completă și $c : L \to L$ operatorul de închidere asociat. Submulțimea C este Z-completă dacă și numai dacă operatorul c este Z-continuu.*

Demonstrație. Presupunem că mulțimea C este Z-completă. Deoarece c este aplicație izotonă, rezultă că $\forall\, A \in Z_L$ avem $c(\sup A) \geqslant \sup c(A)$. Rămîne de arătat că $c(\sup A) \leqslant \sup c(A)$. Dar $\forall\, a \in A$, $a \leqslant c(a) \leqslant \sup c(A)$, deci $\sup A \leqslant \sup c(A)$ și $c(\sup A) \leqslant c(\sup c(A))$. Dar c este izoton și ca atare $c(A) \in Z_L$; cum $c(A) \subset C$, rezultă că $\sup c(A) \in C$, adică $c(\sup c(A)) = \sup c(A)$.

Reciproc, să presupunem că operatorul c este Z-continuu, deci $\forall A \in Z_L$, $A \subset C$ avem $\sup c(A) = c(\sup A) \in C$. Dar $c(A) \supset A$ și ca atare $\sup A \in C$. ∎

Sisteme de închidere

Fie E o mulțime. Reamintim că se numește *sistem de închidere* pe E orice parte inf-completă a lui $\mathbf{p}(E)$.

Fie $\mathcal{C} \subset \mathbf{p}(E)$ un sistem de închidere pe E. Atunci $E \in \mathcal{C}$ și intersecția oricărei familii de mulțimi din $\mathcal{C}$ aparține lui $\mathcal{C}$. Fie $c : \mathbf{p}(E) \to \mathbf{p}(E)$ operatorul de închidere asociat lui $\mathcal{C}$, conform teoremei 4.3. Vom nota pentru orice $A \subset E$, $\bar{A}$ în loc de $c(A)$: conform lemei 1, d), rezultă

$$\bar{A} = \bigcap_{I \in \mathcal{C},\, I \supset A} I.$$

Vom pune $\bar{x}$ în loc de $\overline{\{x\}}$ pentru $x \in E$. Atunci $\forall I \in C$, avem $I = \bigcup_{x \in I} \bar{x}$.

Exemplu. Dacă X este un spațiu metric, atunci submulțimile închise ale lui X sînt elementele unui sistem de închidere pe X, ceea ce justifică terminologia utilizată.

Sisteme de închidere Z-complete și latici Z-izolat generate

Un sistem de închidere $\mathcal{C}$ pe o mulțime E se numește *T_0-separat* dacă $\forall x, y \in E$, $x \neq y$, $\exists I \in \mathcal{C}$ astfel încît $x \in I$, $y \notin I$ sau $x \notin I$, $y \in I$. Această proprietate este echivalentă cu:

$$\forall x, y \in E, \quad \bar{x} = \bar{y} \Rightarrow x = y.$$

Sistemele de închidere sînt în particular latici complete și se pune problema caracterizării sistemelor de închidere Z-complete ca latici complete.

Să fixăm un sistem Z de părți și o latice completă L. Un element $i \in L$ se numește *Z-izolat* dacă pentru orice $A \in Z_L$, din faptul că $i \leqslant \sup A$ rezultă că există $a \in A$ astfel încît $i \leqslant a$.

Vom nota $I^Z \subset L$ mulțimea elementelor Z-izolate; în plus, pentru orice $x \in L$, punem

$$I^Z_x = \{i \in I^Z \mid i \leqslant x\}.$$

LEMA 2. a) $\forall x, y \in L$, $x \leqslant y \Rightarrow I^Z_x \subset I^Z_y$;

b) $\forall A \subset L$, $\bigcap_{x \in A} I^Z_x = I^Z_{\inf A}$;

c) $\forall A \in Z_L$, $\bigcup_{x \in A} I^Z_x = I^Z_{\sup A}$.

Demonstrație. a) Dacă $x \leqslant y$ și $i \in I^Z_x$, atunci $i \leqslant x$, deci $i \leqslant y$, adică $i \in I^Z_y$.

b) Conform cu a) avem $I^Z_{\inf A} \subset I^Z_x$ pentru orice $x \in A$, deci $I^Z_{\inf A} \subset \bigcap_{x \in A} I^Z_x$. Apoi, dacă $x \in A$, $i \in I^Z_x$, atunci $i \leqslant x$, deci $i \leqslant \inf A$ și ca atare $i \in I^Z_{\inf A}$.

c) Conform a) avem $\forall x \in A$, $I^Z_x \subset I^Z_{\sup A}$, deci $\bigcup_{x \in A} I^Z_x \subset I^Z_{\sup A}$. Invers, $\forall i \in I^Z_{\sup A}$ avem $i \leqslant \sup A$, deci există $a \in A$, $i \leqslant a$, adică $i \in I^Z_a \subset \bigcup_{x \in A} I^Z_x$. ∎

Laticea L se numește *Z-izolat generată* dacă $\forall x \in L$, $\exists A \subset I^Z$ astfel încît $x = \sup A$, ceea ce este echivalent cu : $\forall x \in L$, $x = \sup I^Z_x$ (căci dacă $A \subset I^Z$ și $x = \sup A$, atunci $A \subset I^Z_x$).

TEOREMA 4.4. a) *Orice sistem de închidere Z-complet este o latice completă Z-izolat generată.*

b) *Orice latice completă Z-izolat generată este izomorfă cu un sistem de închidere Z-complet și T_0-separat.*

Demonstrație. a) Fie $\mathcal{C} \subset \mathbf{p}(E)$ un sistem de închidere, parte Z-completă a lui $\mathbf{p}(E)$. Arătăm mai întîi că $\forall x \in E$, $\bar{x}$ este Z-izolat în $\mathcal{C}$. Fie $\mathcal{A} \subset \mathcal{C}$ o Z-parte a lui $\mathbf{p}(E)$ astfel încît $\bar{x} \subset \sup_{\mathcal{C}} \mathcal{A}$. Deoarece $\mathcal{C}$ este Z-complet rezultă că $\sup_{\mathcal{C}} \mathcal{A} = \bigcup_{I \in \mathcal{A}} I$. Cum $x \in \bar{x}$, rezultă $x \in \bigcup_{I \in \mathcal{A}} I$, deci există $I \in \mathcal{A}$ astfel încît $x \in I$, de unde $\bar{x} \subset I$.

Rămîne să arătăm că orice $I \in \mathcal{C}$ se exprimă ca margine superioară de elemente Z-izolate. Dar $I = \bigcup_{x \in I} \bar{x}$ și cum $I \in \mathcal{C}$, rezultă $I = \bar{I} = \bigcup_{x \in I} \bar{x} = \sup_{\mathcal{C}} \{\bar{x}\}$.

b) Fie L o latice completă Z-izolat generată și $\mathcal{C} = \{I^Z_x\}_{x \in L} \subset \mathbf{p}(I^Z)$. Observăm că $I^Z_x \subset I^Z_y$, deci $x = \sup^Z_x \leqslant \sup^Z_y = y$. Ținînd cont de lema 2, a), rezultă că există o bijecție izotonă, cu inversa izotonă, între L și $\mathcal{C}$, anume $\varphi : L \to \mathcal{C}$, $x \mapsto \sup I^Z_x$. Fie $\mathcal{A} \subset \mathcal{C}$: conform lemei 2, b) avem

$$\bigcap_{I \in \mathcal{A}} I = \bigcap_{x \in \varphi^{-1}(\mathcal{A})} \varphi(x) = \bigcap_{x \in A} I^Z_x = I^Z_{\inf A} = \varphi(\inf A) \in \mathcal{C},$$

unde $A = \varphi^{-1}(\mathcal{A})$. Fie acum $\mathcal{A} \subset \mathcal{C}$ și A o Z-parte a lui $\mathbf{p}(I^Z)$. Deoarece $\mathcal{A} = c(A)$, unde $c : \mathbf{p}(I^Z) \to \mathcal{C}$ este restricția operatorului de închidere asociat lui $\mathcal{C}$, ținînd cont că operatorul c este continuu (conform corolarului 1, b) al teoremei 4.3), deci și izoton, rezultă că A este de asemenea o Z-parte a lui $\mathcal{C}$. Așadar, $A = \varphi^{-1}(\mathcal{A})$ este o Z-parte a lui L (deoarece φ^{-1} este izotonă). Prin urmare,

$$\bigcup_{I \in \mathcal{A}} I = \bigcup_{x \in \varphi^{-1}(\mathcal{A})} \varphi(x) = \bigcup_{x \in A} I^Z_x = I^Z_{\sup A} = \varphi(\sup A) \in \mathcal{C}.$$

conform lemei 2, c). Dacă $x \in I^z$, atunci $x \in I_x^z$ și $\forall I = I_y^z \in \mathcal{C}$ astfel încît $x \in I$, rezultă $x \leqslant y$, deci $I_x^z \subset I_y^z = I$, adică $I_x^z = \tilde{x}$. În concluzie, dacă $x, y \in I^z$ și $\bar{x} = \bar{y}$, atunci $x = \sup \bar{x} = \sup \bar{y} = y$ și sistemul de închidere $\mathcal{C}$ rezultă T_0-separat. ∎

Rezultatele de mai sus pot fi aplicate sistemelor de închidere **p**-complete, adică supratopologiilor. Sistemele de închidere Δ-complete se mai numesc *sisteme de închidere algebrice* (deoarece subalgebrele unei Ω-algebre fixate peste o signatură Ω formează un sistem de închidere algebric), iar laticile complete Δ-izolat generate se numesc *latici algebrice*. Sistemele de închidere **f**-complete sînt de fapt închiși ai unei topologii și de aceea se mai numesc *sisteme de închidere topologice*, iar laticile complete **f**-izolat generate se numesc *latici topologice*.

§ 4.2. OPERATORI IZOTONI ȘI SUPRATOPOLOGII

La începutul acestui paragraf vom stabili un nou rezultat de inducție și vom studia operatorul de închidere generat de un operator izoton.

Ca aplicație vom stabili cîteva legături între supratopologii și unele concepte algebrice.

Un principiu general de inducție

Fixăm o latice completă L și un operator izoton $\varphi : L \to L$. Vom nota

$$S_\varphi = \{x \in L \mid \varphi(x) \leqslant x\},$$

mulțimea punctelor *superior fixe* ale lui φ.

LEMA 3. *S_φ este o parte inf-completă a lui L.*

Demonstrație. Pentru orice $A \subset S_\varphi$ și oricare ar fi $x \in A$, avem $\inf A \leqslant x$. Deci $\varphi(\inf A) \leqslant \varphi(x) \leqslant x$ și ca atare $\varphi(\inf A) \leqslant \inf A$, adică $\inf A \in S_\varphi$. ∎

Teorema care urmează este un principiu de inducție (inițializare și dinamică) într-o latice completă.

TEOREMA 4.5. *(principiu de inducție în raport cu x_0 și φ). Fie $(L, \leqslant)$ o latice completă, $\varphi : L \to L$ un operator izoton și $x_0 \in L$ fixat. Notăm cu c_φ operatorul de închidere asociat lui S_φ (conform teoremei 4.3). Atunci pentru orice $x \in L$ astfel încît:*

1) $x_0 \leqslant x$ *(baza de inducție)*;

2) $\varphi(x) \leqslant x$ *(pasul de inducție)*,

rezultă $c_\varphi(x_0) \leqslant x$.

Demonstrație. Deoarece $C = S_\varphi$ este o parte inf-completă, operatorul de închidere asociat ei este

$$c_\varphi : L \to L, \qquad x \mapsto \inf C_x,$$

unde $C_x = \{y \in S_\varphi \mid y \geq x\}$. În particular, rezultă $C_{x_0} = \{y \in L \mid \varphi(y) \leq y,\ x_0 \leq y\}$ și din faptul că $x_0 \leq x$, $\varphi(x) \leq x$, se deduce că $x \in C_{x_0}$. Așadar, $c_\varphi(x_0) = \inf C_{x_0} \leq x$. ■

Exemplu. Fie laticea $L = \mathfrak{p}(\mathbb{N})$, cu ordinea dată de incluziune, $x_0 = \{0\}$ și $s : L \to L$, $A \mapsto s(A) = \{x+1 \mid x \in A\}$. Evident, s este un operator izoton și $C_{x_0} = \{B \subset \mathbb{N} \mid s(B) \subset B,\ 0 \in B\} = \mathbb{N}$. Pentru orice $A \in L$ astfel încît $0 \in A$, $s(A) \subset A$, teorema 4.5 arată că $\mathbb{N} \subset A$, adică $A = \mathbb{N}$.

COROLAR 1. *Fie L, φ ca în enunțul teoremei 4.5. Atunci pentru orice $a \in L$, $c_\varphi(a)$ este cea mai mică soluție a ecuației $x = a \vee \varphi(x)$* (pentru p, $q \in L$ se notează $p \vee q = \sup\{p, q\}$).

Demonstrație. Fie $\bar{a} = c_\varphi(a)$ și $a' = a \vee \varphi(\bar{a})$. Avem $a \leq \bar{a}$ și $\bar{a} \in S_\varphi$, deci $\varphi(\bar{a}) \leq \bar{a}$, adică $a' \leq \bar{a}$. Apoi, $\varphi(a') \leq \varphi(\bar{a}) \leq a'$. Deoarece $a \leq a'$ și $\varphi(a') \leq a'$, conform teoremei 4.5, rezultă $c_\varphi(a) \leq a'$, adică $\bar{a} \leq a'$. Ca atare $\bar{a} = a'$ și deci $a \vee \varphi(\bar{a}) = \bar{a}$, adică $\bar{a}$ este o soluție a ecuației din enunț. Dacă x este o altă soluție, atunci $a \leq x$, $\varphi(x) \leq x$ și, conform teoremei 4.5, avem $\bar{a} \leq x$. ■

COROLAR 2. *Fie L, φ ca în enunțul teoremei 4.5. Atunci c_φ este cel mai mic operator extensiv și preidempotent (adică $c^2 \leq c$) astfel încît $\varphi \leq c_\varphi$.* [Dacă $u, v : X \to M$ sînt funcții cu valori într-o m.o. $(M, \leq)$, atunci se scrie $u \leq v$ dacă $u(x) \leq v(x)$ pentru orice $x \in X$.]

Demonstrație. Arătăm mai întîi că $\varphi \leq c_\varphi$. Fie $\forall\, x \in L$. Atunci $c_\varphi(x) \in S_\varphi$, deci $\varphi(c_\varphi(x)) \leq c_\varphi(x)$. Dar $x \leq c_\varphi(x)$, deci $\varphi(x) \leq \varphi(c_\varphi(x)) \leq c_\varphi(x)$. Fie apoi $\psi : L \to L$ un operator extensiv și idempotent astfel încît $\varphi \leq \psi$. Atunci $\forall\, x \in L$, $\varphi(\psi(x)) \leq \psi(\psi(x)) \leq \psi(x)$ și cum $x \leq \psi(x)$ teorema 4.5 arată că $c_\varphi(x) \leq \psi(x)$, adică $c_\varphi \leq \psi$. ■

Operatorul de închidere generat de un operator izoton

În general, dacă M este o m.o. și L o latice completă, atunci mulțimea $\mathfrak{I}$ a funcțiilor izotone $M \to L$ este o sublatice a laticii complete L^M [Pentru orice $f, g \in L^M$ se pune $f \leq g \leftrightarrow \forall\, m \in M$, $f(m) \leq g(m)$; se obține o relație de ordine pe mulțimea L^M și, în plus, L^M este o latice completă: pentru orice $\mathfrak{F} \subset L^M$, $\sup \mathfrak{F}$ este funcția $M \to L$, $m \mapsto \sup_{f \in \mathfrak{F}} f(m)$, iar $\inf \mathfrak{F}$ este funcția $M \to L$, $m \mapsto \inf_{f \in \mathfrak{F}} f(m)$.]

Operatorul de închidere asociat lui $\mathfrak{I}$, $c_{\mathfrak{I}} : L^M \to L^M$, $f \mapsto c_{\mathfrak{I}}(f)$, este definit prin

$$c_{\mathfrak{I}}(f)(x) = \sup_{y \leq x} f(y), \qquad \forall\, x \in M.$$

Operatorul de deschidere asociat lui $\mathfrak{I}$ este $o_{\mathfrak{I}} : L^M \to L^M$, definit prin

$$o_{\mathfrak{I}}(f)(x) = \inf_{y \geq x} f(y), \qquad \forall\, f \in L^M, \qquad \forall\, x \in M.$$

Dacă $M = L$, atunci vom nota cu $\mathfrak{I}_L$ mulțimea operatorilor izotoni ai lui L (care este o sublatice a lui L^L, deci o latice completă). Conform corolarului 2 al teoremei 4.5, *mulțimea operatorilor de închidere ai lui L este o parte inf-completă a laticii complete $\mathfrak{I}_L$*. În mod dual, *mulțimea operatorilor de deschidere ai lui L este o parte sup-completă a laticii complete $\mathfrak{I}_L$*.

În cazul cînd φ satisface condiții suplimentare, acestea se reflectă și asupra lui c_φ. În acest sens are loc următorul rezultat.

Teorema 4.6. *Fie L o latice completă și $\varphi : L \to L$ un operator izoton.*

a) *Pentru orice sistem de părți Z, dacă operatorul φ este Z-continuu, atunci S_φ este o parte Z-completă și c_φ este Z-continuu.*

b) *Dacă φ este continuu, atunci*

$$c_\varphi = \sup_{n \geqslant 0} \varphi^n (\varphi^0 = 1_L, \ \varphi^{n+1} = \varphi^n \circ \varphi).$$

Demonstrație. a) Fie $A \in Z_L$, $A \subset S_\varphi$. Atunci $\forall\, a \in A$, $\varphi(a) \leqslant a \leqslant \sup A$, deci $\sup \varphi(A) \leqslant \sup A$. Deoarece φ este Z-continuu, rezultă că $\varphi(\sup A) = \sup \varphi(A) \leqslant \sup A$, adică $\sup A \in S_\varphi$.

b) Să notăm $\varphi^* = \sup\limits_{n \geqslant 0} \varphi^n$ și fie $x_0 \in L$. Vom arăta că $\varphi^*(x_0)$ *este cel mai mic element al mulțimii* $(S_\varphi)_{x_0}$. Într-adevăr, să observăm mai întîi că $x_0 = 1_L(x_0) = \varphi^0(x_0) \leqslant \sup\limits_{n \geqslant 0} \varphi^n(x_0) = \varphi^*(x_0)$, deci $\varphi(\varphi^*(x_0)) = \varphi(\sup\limits_{n \geqslant 0} \varphi^n(x_0)) = \sup\limits_{n \geqslant 0} \varphi^{n+1}(x_0) \leqslant 1_L \vee \sup\limits_{n \geqslant 0} \varphi^{n+1}(x_0) = \varphi^*(x_0)$, φ fiind continuă. Așadar, $\varphi^*(x_0) \in (S_\varphi)_{x_0}$. Pe de altă parte, $\forall\, x \in (S_\varphi)_{x_0}$, avem $x_0 \leqslant x$ și $\varphi(x) \leqslant x$. Prin inducție după n se arată ușor că $\forall\, n \geqslant 0$, $\varphi^n(x_0) \leqslant x$ [Pentru $n = 0$, $x_0 \leqslant x$, iar dacă $\varphi^n(x_0) \leqslant x$, atunci $\varphi^{n+1}(x_0) = \varphi(\varphi^n(x_0)) \leqslant \varphi(x) \leqslant x$.] Așadar, $\sup\limits_{n \geqslant 0} \varphi^n(x_0) \leqslant x$, adică $\varphi^*(x_0) \leqslant x$. În concluzie, $\varphi^*(x_0)$ este cel mai mic element al lui $(S_\varphi)_{x_0}$, deci, conform lemei 1, $\varphi^*(x_0) = c_\varphi(x_0)$. ■

Supratopologii (cf. [7])

Fixăm o mulțime nevidă X; reamintim că o *supratopologie pe X* este o familie σ de părți ale lui X (numite *părți deschise* sau *deschiși*), stabilă la intersecții și reuniuni arbitrare. Familia mulțimilor închise, adică

$$\sigma^c = \{I \subset X \mid X \setminus I \in \sigma\}$$

este de asemenea o supratopologie pe X, numită duala lui σ; evident, $(\sigma^c)^c = \sigma$.

Exemple. Fiind dată o $\mathbb{1}$-dinamică $A, f : A \to A$, subdinamicile ei (părți $B \subset A$ astfel încît $f(B) \subset B$) formează o supratopologie pe A, deoarece pentru orice familie $\{B_i\}_{i \in I}$

de părți ale lui A astfel încît $\forall\, i \in I$, $f(B_i) \subset B_i$, rezultă că $f(\bigcap_{i\in I} B_i) \subset \bigcap_{i\in I} B_i$ și $f(\bigcup_{i\in I} B_i) \subset \bigcup_{i\in I} B_i$. În particular, subsistemele iterative ale unui sistem iterativ (în sensul definiției 3.16) formează o supratopologie.

Multe alte exemple de supratopologii sînt obținute pornind de la relații binare și algebre unare sau sînt legate de latici complete, așa cum vom vedea în continuare. De exemplu, dacă ρ este o relație binară pe X, atunci

$$\sigma = \{U \subset X \mid \forall\, x,\ y \in X,\ x\,\rho\, y,\ x \in U \Rightarrow y \in U\}$$

este o supratopologie pe X.

Un spațiu supratopologic (X, σ) este o mulțime nevidă X împreună cu o supratopologie σ pe X. Pentru orice parte $A \subset X$ vom nota

$$\bar{A} = \bigcap_{I \supset A,\ I \in \sigma^c} I \quad \text{și} \quad \underline{A} = \bigcap_{U \supset A,\ U \in \sigma} U.$$

Dacă $x \in X$, atunci se notează $\bar{x}$ (resp. $\underline{x}$) în loc de $\overline{\{x\}}$ (resp. $\underline{\{x\}}$). O supratopologie este *T_0-separată* (sau, pe scurt, T_0) dacă $\forall\, x, y \in X$, $\underline{x} = \underline{y} \Rightarrow x = y$.

Exemplu. Fie $X = \mathbb{N}$; șirul $\{S_n\}_{n\geqslant 0}$ de părți ale lui $\mathbb{N}$, $S_n = \{x \in \mathbb{N} \mid x < n\}$, la care adăugăm $\mathbb{N}$, formează o supratopologie pe $\mathbb{N}$. Pentru orice $n \in \mathbb{N}$ avem

$$\underline{n} = S_{n+1} \quad \text{și} \quad \bar{n} = n\}.$$

Această supratopologie este evident T_0-separată.

Pentru orice parte $A \subset X$ avem $\bar{A} = \bigcup_{x\in A} \bar{x}$, $\underline{A} = \bigcup_{x\in A} \underline{x}$; dacă $A \in \sigma$, atunci $A = \bigcup_{x\in A} x$, iar dacă $A \in \sigma^c$, $A = \bigcup_{x\in A} \bar{x}$. Este evident că două supratopologii σ, σ' pe X sînt egale $\leftrightarrow \underline{x}$ (în σ) $= \underline{x}$ (în σ') pentru orice $x \in X$. Dacă (X, σ) și (Y, τ) sînt două spații supratopologice, o aplicație $f : X \to Y$ se numește continuă dacă $\forall\, V \subset Y$, $V \in \tau \Rightarrow f^{-1}(V) \in \sigma$. Dacă f este bijectivă și f, f^{-1} sînt continue, se spune că f este un *homeomorfism.*

Supratopologii și relații binare

Reamintim că dacă X și Y sînt două mulțimi, a defini o relație binară de la X la Y revine la a fixa o parte $\rho \subset X \times Y$; se mai scrie $\rho : X \to Y$ (definiția 1.1). Oricărei relații $\rho : X \to Y$ i se poate asocia *funcția de luare a imaginii directe:*

$$\rho^{\sim} : \mathbf{p}(X) \to \mathbf{p}(Y),\ A \mapsto \tilde{\rho}(A) = \{y \in Y \mid \exists\, x \in A \text{ astfel ca } x\,\rho\, y\}.$$

Pentru orice familie $\{A_i\}_{i\in I}$ de părți ale lui X, avem

$$\tilde{\rho}\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} \tilde{\rho}(A_i),$$

deci aplicația $\rho^\sim$, notată și $\tilde{\rho}$, este continuă. Reținem că $x\rho y \leftrightarrow y \in \tilde{\rho}(\{x\})$.

Dacă $f : \mathbf{p}(X) \to \mathbf{p}(Y)$ este o funcție continuă, atunci se poate defini relația $\rho : X \to Y$ prin $x\rho y \leftrightarrow y \in f(\{x\})$ și se observă că $f = \rho^\sim$. Am stabilit astfel o corespondență bijectivă

$$\mathbf{Rel}(X, Y) \to \mathbf{C}(\mathbf{p}(X), \mathbf{p}(Y)), \quad \rho \mapsto \rho^\sim$$

(**Rel** este categoria având ca obiecte mulțimile iar ca morfisme — relațiile între mulțimi, iar $\mathbf{C} = \mathbf{C}_p$ este categoria laticilor complete și aplicațiilor continue. Reamintim totodată convenția după care pentru orice categorie $\mathbf{C}$ și pentru orice două obiecte X, $Y \in \mathrm{Ob}\,\mathbf{C}$ se notează $\mathbf{C}(X, Y)$ mulțimea morfismelor în $\mathbf{C}$ de la X la Y).

Cu notații și în condiții ușor de explicitat, au loc următoarele *proprietăți ale imaginilor directe*:

— $(\rho_1 \circ \rho)^\sim = \rho_1^\sim \circ \rho^\sim$;

— $(1_X)^\sim = 1_{\mathbf{p}(X)}$;

— $\rho \subset \rho_1 \leftrightarrow \tilde{\rho} \subset \tilde{\rho_1}$ (deci corespondența bijectivă anterioară este izotonă);

— $\left(\bigcup_{i\in I} \rho_i\right)^\sim = \sup_{i\in I} \rho_i^\sim$.

De aici și direct din definiții, rezultă următoarele proprietăți:

— relația $\rho \subset X^2$ este reflexivă $\leftrightarrow \rho^\sim$ este operator extensiv al lui $\mathbf{p}(X)$;

— relația $\rho \subset X^2$ este tranzitivă $\leftrightarrow \rho^\sim$ este operator preidempotent al lui $\mathbf{p}(X)$, adică $\rho^\sim \circ \rho^\sim \subset \rho^\sim$;

— ρ este o relație de preordine pe $X \leftrightarrow \rho^\sim$ este operator de închidere continuu al lui $\mathbf{p}(X)$;

— $(\rho^*)^\sim = (\rho^\sim)^*$ [ρ^* este închiderea reflexivă și tranzitivă a relației ρ, definită în § 1.3, iar $(\rho^\sim)^*$ este operatorul de închidere generat de operatorul continuu $\rho^\sim$, adică tocmai $c_{\rho^\sim}$; conform teoremei 4.6, avem $(\rho^\sim)^* = \sup_{n\geqslant 0} (\rho^\sim)^n$].

Să fixăm o mulțime X și fie $\rho \in \mathbf{Rel}(X)$. Operatorului continuu $\rho^\sim : \mathbf{p}(X) \to \mathbf{p}(X)$ îi corespunde o sublatice a lui $\mathbf{p}(X)$, adică o supratopologie pe X, pe care o vom nota cu σ. Așadar, pentru $U \subset X$,

$$U \in \sigma \leftrightarrow \rho^\sim(U) \subset U, \text{ adică } \forall\, x, y \in X,\ x\rho y,\ x \in U \Rightarrow y \in U.$$

Reciproc, *dacă σ este o supratopologie pe X, atunci se poate considera relația* ρ_1, definită prin:

$$\forall\, x, y \in X, \quad x\rho_1 y \leftrightarrow U \in \sigma, \{x \in U \Rightarrow y \in U\}.$$

Dacă se notează prin $c : \mathbf{p}(X) \to \mathbf{p}(X)$ operatorul de închidere continuu asociat lui σ (conform teoremei 4.6), atunci $x \rho_1 y \leftrightarrow y \in c(\{x\})$, ceea ce rezultă din egalitatea

$$c(\{x\}) = \bigcap_{U \in \sigma,\, x \in U} U.$$

Conform celor spuse mai sus, c este de forma $\pi^{\sim}$, unde π este o relație de preordine și $\rho_1 = \pi$, deci ρ_1 este o preordine.

În cazul cînd ρ este o relație binară pe X, σ este supratopologia pe X asociată lui ρ (c fiind operatorul de închidere continuu asociat) și ρ_1 preordinea asociată lui σ, atunci $\rho_1 = \rho^*$, iar dacă ρ este o preordine, atunci $\rho_1 = \rho$ [căci $c = (\rho^{\sim})^* = (\rho^*)^{\sim} = \rho_1^{\sim}$, de unde $\rho_1 = \rho^*$]. Așadar, *există o corespondență bijectivă între relațiile de preordine pe X și supratopologiile pe X*. Dacă preordinea ρ și supratopologia σ corespund una celeilalte, vom scrie pe scurt $\rho \mid \sigma$.

Dacă σ este o supratopologie pe X, atunci $\sigma^c = \{F \mid X \setminus F \in \sigma\}$ este de asemenea o supratopologie (deci conceptul de supratopologie este autodual). Pînă acum am interpretat elementele sistemelor de închidere (topologice, de pildă) ca închiși. În cazul supratopologiilor, care sînt un caz special de topologii, din cauza autodualității vom adopta terminologia utilizată în topologia generală. Iată o listă de proprietăți de ordine și proprietăți topologice conectate între ele prin corespondența bijectivă evidențiată mai sus (fără a mai da detalii de demonstrație):

— $\rho \mid \sigma \leftrightarrow \rho^{-1} \mid \sigma^c$;

— dacă $f : X \to X'$, $\rho \mid \sigma$ pe X și $\rho' \mid \sigma'$ pe X', atunci f este (σ, σ')-continuă în sens topologic $(V \in \sigma' \Rightarrow f^{-1}(V) \in \sigma) \leftrightarrow f$ este (ρ, ρ')-izotonă $(x \rho y \Rightarrow f(x) \rho' f(y))$;

Să presupunem acum că $\rho \mid \sigma$ pe X. Atunci:

— ρ este o relație de ordine parțială $\leftrightarrow \sigma$ este T_0-separată;

— o relație de ordine ρ este liniară ($\forall\, x, y \in X$, $x \rho y$ sau $y \rho x$) $\leftrightarrow$ $\leftrightarrow \sigma$ este un lanț (**l**-parte) în $\mathbf{p}(X)$;

— relația de ordine ρ are proprietatea că orice parte nevidă are un cel mai mic element $\leftrightarrow \sigma$ este T_0 și orice deschis $U \in \sigma$ are punct generic (adică $\exists\, x \in U$ astfel ca $U = \underline{x}$);

— relația $(\rho \cup \rho^{-1})^*$ este liniară $\leftrightarrow (X, \overline{\sigma})$ este conex;

— (X, ρ) este dirijată (adică $\forall\, x, y \in X, \exists\, z \in X$, $x \rho z, y \rho z$) $\leftrightarrow$ $\leftrightarrow (X, \sigma)$ este ireductibil (adică $\forall\, F_1, F_2 \subset X$ închiși, $F_1, F_2 \in \sigma^c$ și $X = F_1 \cup F_2 \Rightarrow X = F_1$ sau $X = F_2$).

Supratopologii și algebre unare

Fie X o algebră unară (adică o $\mathfrak{U}$-algebră unde $\mathfrak{U}$ este o signatură formată din simboluri de operații unare pe X). Mulțimea subalgebrelor lui X, adică

$$\{U \subset X \mid f(U) \subset U \text{ pentru orice } f : X \to X,\ f \in \mathfrak{U}\}$$

este în mod evident o supratopologie pe X, notată $\sigma_{\mathfrak{U}}$.

Pentru orice supratopologie σ pe X considerăm familia de operații unare

$$\mathfrak{U}(\sigma) = \{f \in X^X \mid f(U) \subset U \text{ pentru orice deschis } U \in \sigma\}.$$

Evident, $\mathfrak{U}(\sigma)$ este un submonoid al monoidului $(X^X, \circ, 1_X)$.

De asemenea, pentru orice parte $\mathfrak{U} \subset X^X$ notăm cu $\overline{\mathfrak{U}}$ submonoidul generat de $\mathfrak{U}$ și $\forall\, x \in X$, punem $\overline{\mathfrak{U}}(x) = \{y \in X \mid \exists\, f \in \overline{\mathfrak{U}}$ astfel încît $y = f(x)\}$.

Au loc următoarele proprietăți :

— $\forall\, x \in X$, $\underline{x}$ (în $\sigma_{\mathfrak{U}}$) $= \overline{\mathfrak{U}}(x)$;

— $\sigma_{\mathfrak{U}} = \sigma_{\overline{\mathfrak{U}}}$;

— pentru orice supratopologie σ pe X, avem $\sigma = \sigma_{\mathfrak{U}(\sigma)}$ [este suficient de observat că $\underline{x}$ (în σ) $= \mathfrak{U}(\sigma)(x)$].

Ne propunem acum să caracterizăm acele părți $\mathfrak{U} \subset X^X$ astfel încît $\mathfrak{U}(\sigma_{\mathfrak{U}}) = \mathfrak{U}$, adică acele colecții de operații unare pe X care sînt în corespondență bijectivă cu supratopologiile pe X ; în mod necesar $\mathfrak{U}$ este un submonoid al lui X^X, dar nu este suficient. Să considerăm aplicația

$$\partial : (X^X)^X \to X^X, \quad t \mapsto \partial(t),$$

unde pentru orice aplicație $t : X \to X^X$, $\partial(t) : X \to X$ asociază oricărui $x \in X$, elementul $[t(x)](x)$. O mulțime $\mathfrak{U}$ de operații unare pe X se numește *diagonal-închisă* dacă ori de cîte ori $t : X \to X^X$ este o aplicație astfel încît $t(X) \subset \mathfrak{U}$, să rezulte că $\partial(t) \in \mathfrak{U}$. Submulțimile diagonal-închise formează evident un sistem de închidere pe X^X. Notînd cu $\tilde{\mathfrak{U}}$ închiderea diagonală a lui $\mathfrak{U}$ (cea mai mică mulțime diagonal-închisă a lui X^X care conține $\mathfrak{U}$), atunci se pot demonstra ușor următoarele proprietăți :

— pentru orice supratopologie σ pe X, $\mathfrak{U}(\sigma)$ este diagonal-închisă ;

— pentru orice $\mathfrak{U} \subset \Lambda^X$, avem $\mathfrak{U}(\sigma_{\mathfrak{U}}) = \tilde{\mathfrak{U}}$;

— pentru orice $\mathfrak{U} \subset \Lambda^X$ are loc egalitatea $\mathfrak{U}(\sigma_{\mathfrak{U}}) = \mathfrak{U}$ dacă și numai dacă $\mathfrak{U}$ este un submonoid diagonal-închis.

Supratopologii și latici complete

Adaptăm aici cîteva rezultate obținute anterior (teorema 4.4). Evident, *orice supratopologie σ pe o mulțime X este o latice completă* relativ la incluziune. Invers, fie $(L, \leqslant)$ o latice completă și $\perp = \inf L$. Un element $z \in L$ se numește *izolat* dacă $z \neq \perp$ și $\forall A \subset L$, $A \neq \emptyset$, $z \leqslant \sup A \Rightarrow \exists\, a \in A, z \leqslant a$; notăm cu $\operatorname{Is} L$ mulțimea elementelor izolate din L. Pentru orice $x \in L$ considerăm mulțimea $I_x = \{z \in \operatorname{Is} L \mid z \leqslant x\}$.

Evident, pentru orice $A \subset X$,

$$\bigcup_{x \in A} I_x = I_{\sup A}, \quad \bigcap_{x \in A} I_x = I_{\inf A}.$$

Atunci $\mathfrak{I} = \{I_x \mid x \in L\}$ este o supratopologie peste mulțimea $\operatorname{Is} L$, iar spațiul supratopologic $(\operatorname{Is} L, \mathfrak{I})$ se numește *spectrul laticii complete* L ([4]).

Au loc următoarele proprietăți:

— $\forall z \in \operatorname{Is} L$, $\underline{z} = I_z$;

— spectrul unei latici complete este un spațiu T_0;

— orice supratopologie σ pe X este o latice completă și un deschis $U \in \sigma$ este izolat dacă și numai dacă există $x \in U$ astfel încît $U = \underline{x}$;

— aplicația surjectivă $\varphi : X \to \operatorname{Is} \sigma$, $x \mapsto \underline{x}$ este continuă și deschisă (deoarece $\varphi^{-1}(I_U) = U$ și $\varphi(U) = I_U$ pentru orice $U \in \sigma$); în particular, dacă (X, σ) este un spațiu T_0, atunci φ este un homeomorfism;

— un spațiu supratopologic este T_0 dacă și numai dacă el este homeomorf cu spectrul unei latici complete.

O întrebare firească este următoarea: ce latici complete sînt supratopologii? Răspunsul este dat în cele ce urmează. Pentru orice latice completă L și $\forall x \in L$, $I_{\sup I_x} = I_x$. Putem defini atunci aplicația surjectivă

$$\Downarrow : L \to \mathfrak{I}, \quad x \mapsto I_x$$

care este sup-continuă și inf-continuă. Laticea L se numește izolat generată dacă $\forall x \in L$, $\sup I_x = x$. Se verifică imediat că $\Downarrow$ este un izomorfism de latici complete dacă și numai dacă L este izolat generată și că orice supratopologie este o latice completă izolat generată.

Ca o consecință, rezultă că *o latice completă este izomorfă cu o supratopologie dacă și numai dacă ea este izolat generată.*

§ 4.3. PUNCTE FIXE ALE OPERATORILOR IZOTONI

Teorema Knäster-Tarski de punct fix

DEFINIȚIA 4.6. Fie L o latice completă și $\varphi : L \to L$ un operator izoton. Un element $x \in L$ se numește *punct fix* al lui φ dacă $\varphi(x) = x$.

Vom introduce notațiile următoare:

$F_\varphi = \{x \in L \mid \varphi(x) = x\}$ (mulțimea punctelor *fixe* ale lui φ);

$I_\varphi = \{x \in L \mid x \leqslant \varphi(x)\}$ (mulțimea punctelor *inferior fixe*);

$S_\varphi = \{x \in L \mid \varphi(x) \leqslant x\}$ mulțimea punctelor *superior fixe*).

Așadar, $F_\varphi = I_\varphi \cap S_\varphi$. Am văzut (lema 3) că S_φ este o parte inf-completă a lui L. În mod analog se arată că I_φ este o parte sup-completă a lui L.

TEOREMA 4.7 (*Tarski*). *Mulțimea F_φ a punctelor fixe ale unui operator izoton $\varphi : L \to L$ este o latice completă, relativ la ordinea indusă de pe laticea completă L.*

Demonstrație. Mai întîi să observăm că $\varphi(S_\varphi) \subset S_\varphi$. Într-adevăr, $\forall x \in S_\varphi$, $\varphi(x) \leqslant x$, deci $\varphi(\varphi(x)) \leqslant \varphi(x)$, adică $\varphi(x) \in S_\varphi$. În mod similar, $\varphi(I_\varphi) \subset I_\varphi$.

Considerăm operatorul $\psi : S_\varphi \to S_\varphi$, $\psi = \varphi | S_\varphi$ (restricția lui φ). Deoarece S_φ este o latice completă și ψ este izoton (ca și φ), mulțimea I_ψ a punctelor inferior fixe ale lui ψ în S_φ este o parte sup-completă a lui S_φ, deci o latice completă. În mod similar, operatorul $\psi' : I_\varphi \to I_\varphi$, $\psi' = \varphi | I_\varphi$ este izoton și $S_{\psi'}$ este o parte inf-completă a lui I_φ, deci o latice completă. Demonstrația se încheie observînd că $I_\varphi = S_{\psi'} = F_\varphi$. ∎

COROLAR 1 (*Knäster*). *Orice operator izoton într-o latice completă are cel puțin un punct fix.*

Demonstrație. Este suficient să observăm că F_φ este o latice completă; în particular, ea este o mulțime nevidă și are un cel mai mic element.

Se putea observa și direct că S_φ este inf-completă și că există $\min S_\varphi$, acesta fiind cel mai mic punct fix al lui φ. În mod similar, există $\max I_\varphi$ și acesta este cel mai mare punct fix al lui φ. ∎

Observație. **Mulțimea F_φ nu este nici inf-completă și nici sup-completă în L. Totuși „sup" și „inf" se pot exprima cu ajutorul lui „sup", respectiv „inf" în L astfel: pentru orice $A \subset F_\varphi$,**

$$\sup_{F_\varphi} A = \sup_{S_\varphi} A = c_\varphi(\sup_I A); \quad \inf_{F_\varphi} A = \inf_{I_\varphi} A = o_\varphi(\inf_L A),$$

unde $o_\varphi : L \to L$ este operatorul de deschidere asociat părții sup-complete I_φ.

Cel mai mic punct fix al lui φ este $\inf S_\varphi = c_\varphi(\bot)$, iar cel mai mare este $\sup I_\varphi = o_\varphi(\top)$.

Cu notațiile din demonstrația teoremei 4.7. dăm următorul rezultat.

COROLAR 2. *Operatorul de închidere pe I_φ asociat părții inf-complete S_ψ este $c_\varphi|I_\varphi$, iar operatorul de deschidere pe S_φ asociat părții sup-complete I_ψ este $o_\varphi|S_\varphi$.*

Demonstrație. Avem de arătat că $\forall\, x_0 \in I_\varphi$, $\overline{x}_0 = c_\varphi(x_0)$ este cel mai mic punct fix al lui φ, mai mare decît x_0. Evident, $x_0 \leqslant \overline{x}_0$. Deoarece $x_0 \in I_\varphi$, avem $x_0 \leqslant \varphi(x_0) \leqslant \varphi(\overline{x}_0)$. Dar $\overline{x}_0 \in S_\varphi$, deci $\varphi(\overline{x}_0) \leqslant \overline{x}_0$ și $\varphi(\varphi(\overline{x}_0)) \leqslant \varphi(\overline{x}_0)$. Prin inducție în raport cu x_0 și φ (teorema 4.5), rezultă că $\overline{x}_0 \leqslant \varphi(\overline{x}_0)$, deci $\overline{x}_0$ este un punct fix al lui φ.

Pe de altă parte, dacă $x \in F_\varphi$ și $x_0 \leqslant x$, atunci din faptul că $\varphi(x) \leqslant x$ rezultă prin inducție că $\overline{x}_0 \leqslant x$.

În mod similar, $\forall\, x_0 \in S_\varphi$, $o_\varphi(x_0)$ este cel mai mare punct fix, mai mic decît x_0. ∎

O imagine de ansamblu a situației astfel descrise apare în fig. 4.2.

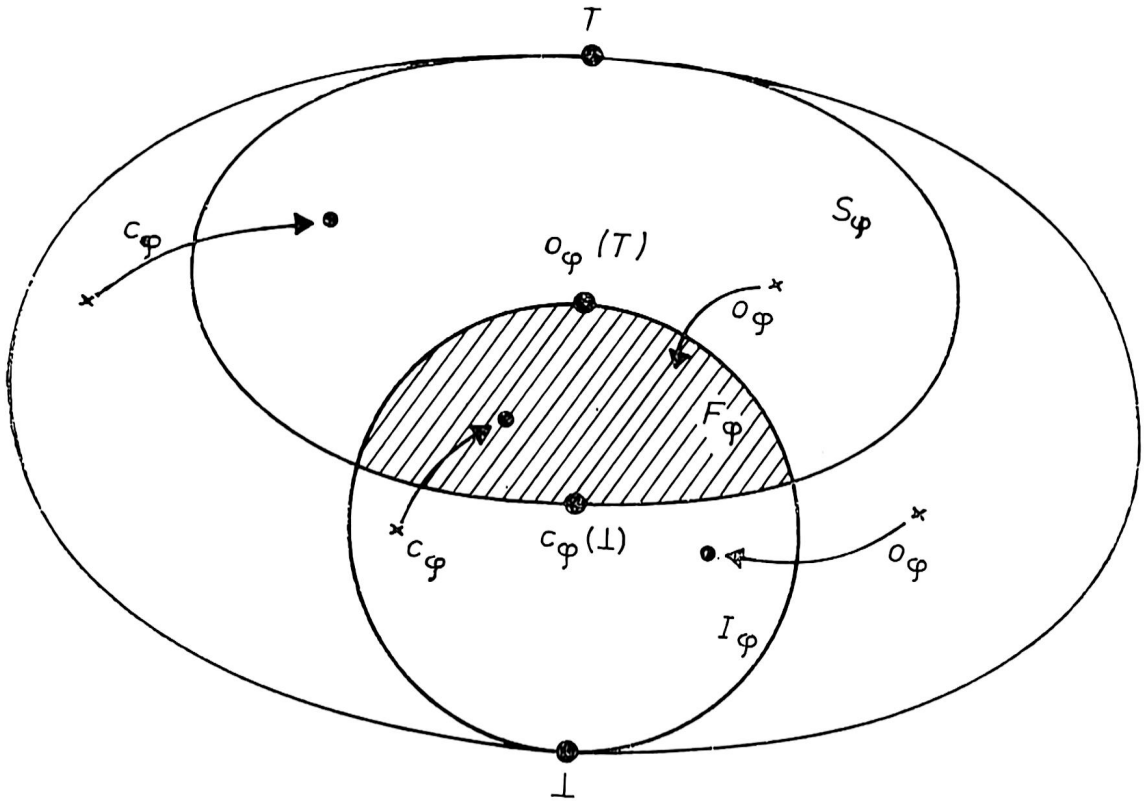


Fig. 4.2

Observație. Fie $(M, \leqslant)$ o mulțime ordonată și $\varphi : M \to M$ o aplicație izotonă. Notăm cu $F_\varphi = \{x \in M \mid \varphi(x) = x\}$ mulțimea punctelor fixe ale lui φ. Se spune că mulțimea ordonată M are proprietatea P.F. dacă pentru orice aplicație izotonă $\varphi : M \to M$, avem $F_\varphi \neq \emptyset$.

Teorema Tarski (4.7) și corolarul 1 al ei arată că o latice completă are proprietatea P.F. și în plus mulțimea punctelor fixe este de asemenea o latice completă. Actualmente asistăm la elaborarea teoriei punctelor fixe pentru mulțimi ordonate oarecare, cu implicații și aplicații importante. De exemplu, dacă B este un spațiu Banach și $T : B \to B$ este un izomorfism liniar continuu, atunci se știe că T^{-1} este de asemenea continuu, deci T

este un automorfism al lui B. Considerînd mulțimea ordonată (relativ la incluziune) $P(B)$ a subspațiilor proprii închise ale lui B, atunci $T : P(B) \to P(B)$ este o aplicație izotonă; punctele ei fixe sînt subspațiile proprii invariante ale operatorului T, care joacă un rol important în analiza funcțională.

Prezentăm fără detalii un rezultat general legat de proprietatea P.F. Fie $(M, \leqslant)$ o mulțime ordonată finită. Notăm cu $\Delta(M)$ complexul simplicial avînd ca vîrfuri elementele lui M și ca simplexe lanțurile din M (de exemplu, $\{x_1 < x_2 < \ldots < x_n\} \subset M$ este un simplex tipic). Notăm cu $|\Delta(M)|$ poliedronul definit de complexul simplicial $\Delta(M)$ și cu $H_q(M, \mathbb{Q})$ grupul de omologie rațională în dimensiunea q a spațiului $|\Delta(M)|$, $H_q(M, \mathbb{Q}) = H_q(|\Delta(M)|; \mathbb{Q})$. Mulțimea ordonată M se numește aciclică dacă $H_q(M, \mathbb{Q}) = 0$ pentru orice $q \in \mathbb{Z}$.

Exemplu. Dacă $|M| = 1$ sau dacă există $x \in M$ comparabil cu orice alt element din M, atunci M este aciclică. Dar mulțimea vidă nu este aciclică (deoarece $H_{-1}(\emptyset, \mathbb{Q}) = \mathbb{Q}$).

Caracteristica Euler-Poincaré a lui M este

$$\mu(M) = \sum_{q \geqslant -1} (-1)^q \dim_{\mathbb{Q}} H_q(M, \mathbb{Q}) = \chi(|\Delta(M)|) - 1,$$

unde $\chi(Z)$ este caracteristica Euler-Poincaré a spațiului Z.

Fie acum $\varphi : M \to M$ o aplicație izotonă. Ea induce o aplicație simplicială $\Delta\varphi : \Delta(M) \to \Delta(M)$ și o aplicație continuă $|\varphi| : |\Delta(M)| \to |\Delta(M)|$, deci φ induce endomorfisme liniare $\varphi_q : H_q(M, \mathbb{Q}) \to H_q(M, \mathbb{Q})$. Are sens să considerăm urmele ν_q ale aplicațiilor φ_q și să definim numărul Lefschetz al lui φ:

$$\lambda(\varphi) = \sum_{q \geqslant 1} (-1)^q \nu_q.$$

Se poate demonstra următoarea teoremă de punct fix de tip Lefschetz: Dacă M este o mulțime ordonată finită și dacă $\varphi : M \to M$ este o aplicație izotonă, atunci $\lambda(\varphi) = \mu(F_\varphi)$. [K. Baclawski, A. Björner, *Fixed points in partially order sets*, Advances in Math. 31 (1979) 263—287]. De aici se deduce următorul fapt remarcabil: *Orice mulțime M ordonată finită și aciclică are proprietatea P.F.*

Într-adevăr, observăm că pentru orice aplicație izotonă $\varphi : M \to M$ avem $\lambda(\varphi) = 0$, deci $\mu(F_\varphi) = 0$ și cum $\mu(\emptyset) = -1$ rezultă că mulțimea F_φ este nevidă.

Rămîn ca probleme de studiu obținerea de criterii suficiente de aciclicitate și extinderea rezultatelor anterioare la mulțimi ordonate infinite.

Puncte fixe ale operatorilor ω-continui

Fie L o latice completă și $\varphi : L \to L$ un operator ω-continuu (reamintim că ω este sistemul de părți care admit numărări izotone, adică sînt imagini izotone ale lui $\mathbb{N}$). În acest caz se poate da o formulare *constructivă* a rezultatului lui Knäster.

Fie $x_0 \in L$ astfel încît $x_0 \leqslant \varphi(x_0)$, adică $x_0 \in I_\varphi$. Conform teoremei 1.1. de inițialitate, există și este unică o funcție $f : \mathbb{N} \to L$ astfel încît $f(0) = x_0$ și $\forall\, n \in \mathbb{N}$, $f(s(n)) = \varphi(f(n))$. Prin inducție după n rezultă că $\forall\, n$, $f(n) \leqslant f(n+1) = \varphi(f(n))$ și că f este izotonă, deci $P = f(\mathbb{N}) = \{\varphi^n(x_0) \mid n \in \mathbb{N}\}$ este o ω-parte a lui L. Fie

$$\overline{x}_0 = \sup P = \sup_{n \geqslant 0} f(n) = \sup_{n \geqslant 0} \varphi^n(x_0).$$

Deoarece $\forall\, n \in \mathbb{N}$, $f(n) \leqslant \varphi(f(n))$, rezultă că $P \subset I_\varphi$ și cum I_φ este sup-completă, atunci $\overline{x}_0 \in I_\varphi$. Apoi, $\forall\, n \in \mathbb{N}$, $\varphi(f(n)) = f(n+1)$, deci $\varphi(P) \subset P$ și ca atare $\sup \varphi(P) \leqslant \sup P$. Deoarece φ este ω-continuă, rezultă $\varphi(\sup P) = \sup \varphi(P) \leqslant \sup P$, deci $\overline{x}_0 = \sup P \in S_\varphi$. Așadar, $\overline{x}_0$ este un punct fix al lui φ. Dacă x este un alt punct fix astfel încît $x_0 \leqslant x$, atunci se verifică imediat prin inducție că $\forall\, n \geqslant 0$, $f(n) \leqslant x$, deci $\overline{x}_0 \leqslant x$. În rezumat am demonstrat teorema următoare.

TEOREMA 4.8. *Dacă L este o latice completă, operatorul $\varphi : L \to L$ este ω-continuu și $x \in L$ este un punct inferior fix al lui φ, atunci $\overline{x} = \sup\limits_{n \geqslant 0} \varphi^n(x)$ este cel mai mic punct fix mai mare decît x. În particular, $\sup\limits_{n \geqslant 0} \varphi^n(\bot)$ este cel mai mic punct fix al lui φ.* ∎

Această teoremă este mai precisă decît rezultatul lui Knäster deoarece dă o expresie constructivă pentru operatorul de închidere asociat lui F_φ în I_φ (în ipoteza că φ este ω-continuu). Din păcate rezultatul nu se extinde și la c_φ, adică la operatorul de închidere asociat lui S_φ în L. În cazul cînd φ este extensiv avem $I_\varphi = L$ și $F_\varphi = S_\varphi$, ceea ce sugerează următoarea construcție: pentru un operator ω-continuu să considerăm $\varphi_1 = \varphi \vee 1_L$, deci $\varphi_1 : L \to L$, $x \mapsto \varphi(x) \vee x$. Se observă că operatorul φ_1 este de asemenea ω-continuu și, în plus, φ_1 este evident extensiv iar $S_\varphi = F_{\varphi_1}$. Așadar, putem da următorul rezultat.

COROLAR. *Fie $\varphi : L \to L$ un operator ω-continuu al unei latici complete L. Atunci $\forall\, x \in L$, $c_\varphi(x) = \sup\limits_{n \geqslant 0} \varphi_1^n(x)$, unde $\varphi_1 = \varphi \vee 1_L$.*

[Altfel spus, $c_\varphi = (\varphi \vee 1_L)^*$, unde am notat $\psi^* = \sup\limits_{n \geqslant 0} \psi^n$.]

Observație. Dacă L este o latice completă și $\varphi : L \to L$ este un operator izoton l-continuu, atunci dăm o demonstrație directă a formulei $\varphi^\uparrow = \inf F_\varphi$ [unde $\varphi^\uparrow = \sup\limits_{n \geqslant 0} \varphi^n(\bot)$; similar se notează $\varphi_\downarrow = \inf\limits_{n \geqslant 0} \varphi^n(\top)$ și se arată că $\varphi_\downarrow = \sup F_\varphi$]. Într-adevăr, să notăm $x_n = \varphi^n(\bot)$, $n \geqslant 0$ și să punem $\varphi = \varphi^\uparrow$. Șirul $\{x_n\}_{n \geqslant 0}$ este evident un lanț și $\varphi(p) = \varphi(\sup\limits_{n \geqslant 0} x_n) = \sup\limits_{n \geqslant 0} \varphi(x_n) = \sup\limits_{n \geqslant 1} x_n = p$, deci $p \in F_\varphi$. Arătăm că $p = \inf F_\varphi$. Este suficient să arătăm că $p \leqslant x$, pentru orice $x \in L$, cu $\varphi(x) \leqslant x$. Cum $p \in F_\varphi$ va rezulta că $p = \inf F_\varphi$. Dar $x_0 = \bot \leqslant x$ și dacă $x_{n-1} \leqslant x$, atunci $x_n = \varphi(x_{n-1}) \leqslant \varphi(x) \leqslant x$, deci $p = \sup\limits_{n \geqslant 0} x_n \leqslant x$; în concluzie, $\varphi^\uparrow = \inf F_\varphi$.

Exemple. 1) Fie (Ω, ν) o signatură și (A, δ) o Ω-algebră (definiția 3.9). Considerăm aplicația $\varphi : \mathfrak{p}(A) \to \mathfrak{p}(A)$ care asociază oricărei părți $M \subset A$, partea $\varphi(M) = \{x \in A \mid |\exists \omega, \nu(\omega) = n, \exists\, m_1, \ldots, m_n \in M$ astfel încît $x = \delta(\omega)(m_1, \ldots, m_n)\}$, adică rezultatele de operații cu argumentele luate din M, inclusiv ale operațiilor nulare. Aceste rezultate pot să nu aparțină lui M.

Aplicația φ este monotonă și ω-continuă. Dacă notăm $\varphi_1 = \varphi \vee 1_{\mathfrak{p}(A)}$, atunci $\forall\, M \subset A$, $\varphi_1(M) = M \cup \varphi(M)$ și punctele fixe ale lui φ_1 sînt tocmai Ω-subalgebrele lui A.

2) Fie X o mulțime și $\rho \in \mathrm{Rel}\, X$ o relație tranzitivă fixată. Considerăm laticea completă $L = \mathrm{Rel}\,(X)$, relativ la incluziune și $\varphi : L \to L$, $R \mapsto \rho \circ R$; φ este un operator ω-continuu și S_φ este mulțimea relațiilor binare R pe X astfel încît $\rho \circ R \subset R$, iar $\overline{\rho} = 1_X \cup \rho \cup \rho^2 \cup \ldots$ este închiderea reflexivă și tranzitivă a lui ρ (punct fix al lui φ).

Aplicație la sistemele discrete

Fixăm o signatură (Ω, ν) în sensul definiției 3.8. Se numește *sistem discret relativ la* Ω orice 5-uplu

$$\mathcal{S}_\Omega = (X, A, h, \gamma, f),$$

unde A este o Ω-algebră (*a stărilor* sistemului), X este o Ω-algebră (*a intrărilor* sau parametrilor de *control*), $h : A \to A$ este un morfism de Ω-algebre, $\gamma \in C(A)$ o congruență pe A și o X-dinamică $f : X \times A \to A$ astfel încît $\forall\, s \in A$, notînd cu $\hat{s}$ clasa de echivalență a lui s modulo γ, să avem $\hat{s} = \{f(x, a) \mid x \in X\}$.

Dacă $x \in X$ este o intrare și $a \in A$ o stare, atunci starea următoare este $f(x, h(a))$. Se mai spune că sistemul $\mathcal{S}_\Omega$ are dinamica discretă $a_{k+1} = f(x_k, h(a_k))$, $k \in \mathbb{Z}$. Remarcăm că pentru orice parametru de control $x \in X$, $f(x, a)$ rămîne în clasa de echivalență (modulo γ) a lui a. Remarcăm de asemenea că nu este specificată o stare inițială.

Exemple. 1) Orice X-dinamică $f : X \times A \to A$ definește un sistem discret relativ la $\Omega = \emptyset$, luînd $h = 1_A$ și $\gamma = A \times A$.

2) Fie A, X spații vectoriale (reale), $h : A \to A$ o aplicație liniară $\gamma : X \to A$ o altă aplicație liniară (definind totodată relația de echivalență $\{(s, t) \in A \times A \mid \exists\, x \in X, s - t = \gamma(x)\}$ și o aplicație $f : X \times A \to A$, $(x, a) \mapsto a + \gamma(x)$; evident, $\{f(x, a) \mid x \in X\} = \{a + \gamma(x) \mid x \in x\} = \hat{a}$. Dinamica sistemului este dată prin $a_{k+1} = h(a_k) + \gamma(x_k)$, $k \in \mathbb{Z}$. Ca un caz particular se obțin sistemele dinamice liniare finit-dimensionale discrete de forma $a_{k+1} = Ca_k + Dx_k$, $k \in \mathbb{Z}$, unde $C \in M_n(\mathbb{R})$, $D \in M_{n,m}(\mathbb{R})$. Luăm $A = \mathbb{R}^n$, $X = \mathbb{R}^m$, $h : \mathbb{R}^n \to \mathbb{R}^n$, $a \mapsto C \cdot a$ (identificînd vectorii din $\mathbb{R}^k$ cu matrici-coloană $k \times 1$); γ = relația binară pe $\mathbb{R}^n$: $a \gamma b \leftrightarrow \exists\, x \in \mathbb{R}^m$ astfel ca $a - b = Dx$ (adică $a - b \in \mathrm{Im}\, D$), iar aplicația $f : X \times A \to A$ este dată prin $f(x, a) = a + D \cdot x$, dinamica sistemului considerat fiind exprimată prin $a_{k+1} = Ca_k + Dx_k$, $k \in \mathbb{Z}$.

Revenim la cazul general. Dacă A este o Ω-algebră, atunci se pot considera laticile complete $S(A)$ și $C(A)$ ale subalgebrelor lui A și, respectiv, congruențelor pe A. Se pot atunci defini două noi operații, notate cu ∇ și cu Δ; anume

$$\nabla : C(A) \times S(A) \to S(A), \quad (\rho, A_1) \mapsto \rho \nabla A_1,$$

unde $\rho \nabla A_1 = \sup \{B \in S(A) \mid \rho(A_1) = \rho(B)\} = \rho^{-1}\rho(A_1)$ [pentru o relație binară $\rho \subset A^2$ și pentru orice $A' \subset A$ punem

$$\rho(A') = \{y \in A \mid \exists\ \ x \in A' \quad \text{astfel încît } x \rho y\}].$$

Relativ la ordinea-produs, aplicația ∇ este izotonă.
Definim apoi

$$\Delta : C(A) \times S(A) \to C(A), \quad (\rho, A_1) \mapsto \rho\Delta A_1,$$

unde $\rho\Delta A_1 = \inf\{\sigma \in C(A) \mid \sigma|A_1 = \rho|A\}$
[dacă $\sigma \subset A^2$ este o relație binară și $A' \subset A$, atunci prin $\sigma|A'$ se înțelege restricția lui σ la A', adică $\sigma \cap (A' \times A')$].
Aplicația Δ este de asemenea izotonă.

Exemplu. Presupunem că A este un spațiu vectorial (real). Orice congruență ρ pe A definește un subspațiu vectorial B al lui A, anume $B = \hat{0}$ și, reciproc, oricărui subspațiu vectorial B al lui A îi corespunde congruența $\rho : \forall\, x, y \in A,\ x\rho y \leftrightarrow x - y \in B$. Așadar, congruențele pe A se identifică prin subspații ale lui A. Cu o astfel de identificare, aplicațiile ∇, Δ sînt definite prin

$$\nabla(T, W) = T + W \quad \text{și} \quad \Delta(T, W) = T \cap W,$$

deci ∇, Δ generalizcază, respectiv, suma și intersecția de supspații ale lui A.

Presupunem acum că Ω admite un simbol nular-0 și fixăm un sistem discret relativ la Ω, $\mathcal{S}_\Omega = (S, A, h, \gamma, f)$; considerăm operatorul izoton al laticii complete $S(A)$ definit prin

$$\varphi : S(A) \to S(A), \quad A_1 \mapsto \gamma\nabla h(A_1).$$

Subalgebra nulă coincide cu $\{\perp\}$ în laticea $S(A)$ și se poate defini *subalgebra de accesibilitate* a sistemului $\mathcal{S}_\Omega$, anume

$$\varphi^\uparrow = \sup_{n \geqslant 0} \varphi^n(\perp).$$

Avem $\varphi^\uparrow \in S(A)$ și $\varphi^\uparrow$ este mulțimea tuturor stărilor accesibile din starea inițială în timp finit, deoarece la orice moment $t \in \mathbb{N}$ mulțimea stărilor accesibile este $\varphi^t(\perp)$.
Deoarece $h : A \to A$ este un morfism de Ω-algebre, rezultă că aplicația $h_S : S(A) \to S(A)$, $A_1 \mapsto h(A_1)$ este $\mathbf{1}$-continuă și aceeași proprietate o are aplicația $\varphi : S(A) \to S(A)$, $A_1 \mapsto \gamma^{-1}\gamma(h(A_1))$. Așadar, $\varphi^\uparrow$ este cel mai mic punct fix al aplicației φ (conform observației de la p. 178).

Exemplu. În cazul sistemelor liniare finit-dimensionale discrete de forma $a_{k+1} = Ca_k + Dx_k$, $k \in \mathbb{Z}$, avem $\varphi : S(A) \to S(A)$, $A_1 \mapsto D + C \cdot A_1$, deci $\forall\, k \geqslant 1$, $\varphi^k(A_1) = D + CD + \ldots + C^{k-1}D + C^kA_1$ și $\varphi^\uparrow = \sum_{k \geqslant 0} C^kD$. Dacă $\dim A = n$, atunci $\varphi^\uparrow$ coincide cu *subspațiul de controlabilitate* $D + CD + \ldots + C^{n-1}D$.

Problema observabilității sistemului $\mathcal{S}_\Omega$ se poate de asemenea pune în context laticial. Fie $\rho \in C(A)$ o congruență pe A și „morfismul de ieșire" $A \to A/\rho$. Două stări $a_0, a_1 \in A$ se numesc *indiscer-*

nabile dacă pentru orice șir de intrare șirurile corespunzătoare de ieșire pornind din stările inițiale a_0, a_1 sînt identice. Considerînd congruența $\rho^* = \inf_{n>0} (\rho \circ h^n)$ [$\forall\, a, b \in A$, $a(\rho \circ h^n)b \leftrightarrow h^n(a)\rho h^n\ (b)$], atunci stările a_0, a_1 sînt indiscernabile dacă și numai dacă $a_0 \rho^* a_1$. Se constată că $\rho^* = (\rho \wedge h_C)_\downarrow$, deci ρ^* este cel mai mare punct fix al aplicației $\rho \wedge h_C : C(A) \to C(A)$, $\sigma \mapsto (\sigma \circ h) \wedge \rho$.

Exemplu. Pentru un sistem liniar finit-dimensional discret $a_{k+1} = Ca_k + Du_k$, $y_k = Rx_k$, congruența ρ^* corespunde subspațiului de observabilitate $\bigcap_{n>0} \mathrm{Ker}\,(R \cdot C^n)$.

Așadar, subspațiile de controlabilitate și observabilitate apar ca puncte fixe ale unor operatori izotoni ai laticilor complete $S(A)$, respectiv, $C(A)$ ([26]).

§ 4.4. MONOIZI COMPLET ORDONAȚI

Noțiunea de monoid complet ordonat

DEFINIȚIA 4.7. Se numește *monoid complet ordonat* orice monoid $(W, \cdot, 1)$ care admite și o structură de latice completă $(W, \leqslant)$ astfel încît pentru orice două părți $A, B \subset W$,

$$\sup (A \cdot B) = (\sup A) \cdot (\sup B).$$

[Am notat $A \cdot B = \{x \cdot y \,|\, x \in A$ și $y \in B\} \subset W$.] Ultima condiție este echivalentă cu faptul că $\forall\, a, b \in W$, $(\sup A)b = \sup (Ab)$ și $a(\sup B) = \sup (aB)$. Notînd $\perp = \sup \emptyset$, atunci pentru $A = \emptyset$ se observă că $\forall\, a \in W$, $\perp \cdot a = \perp$ și $a \cdot \perp = \perp$, deci $\perp$ este un element nul.

Dacă $(W, \cdot, 1)$, $(W', \cdot, 1')$ sînt doi monoizi complet ordonați, prin *morfism de monoizi complet ordonați*, $f : W \to W'$, vom înțelege un morfism continuu de monoizi.

Așadar, $\forall\, w_1, w_2 \in W$, $f(w_1 \cdot w_2) = f(w_1) \cdot f(w_2)$, $f(1) = 1'$ și $\forall\, A \subset W$, $f(\sup A) = \sup f(A)$; în particular, dacă $w_1 \leqslant w_2$ în W, luînd $A = \{w_1, w_2\}$, rezultă $f(w_1) \leqslant f(w_2)$, deci aplicația f este izotonă.

Monoizii complet ordonați și morfismele corespunzătoare formează o categorie, pe care o notăm **Mco**.

Exemple de monoizi complet ordonați

1) Fie $(M, \cdot, e)$ un monoid oarecare și $W = \mathbf{p}(M)$. Pentru orice $A, B \in W$, definim

$$A \cdot B = \{a \cdot b \,|\, a \in A, b \in B\}.$$

Atunci $(W, \cdot, \{e\})$ este un monoid; în plus, W este un monoid complet ordonat deoarece este latice completă și, în plus, pentru orice colecții $\mathcal{A}$, $\mathcal{B}$ de părți ale lui M avem

$$\bigcup_{C \in \mathcal{A} \cdot \mathcal{B}} C = \left(\bigcup_{A \in \mathcal{A}} A\right) \cdot \left(\bigcup_{B \in \mathcal{B}} B\right), \text{ adică } \sup(\mathcal{A} \cdot \mathcal{B}) = (\sup \mathcal{A} \cdot (\sup \mathcal{B}).$$

În particular, dacă X este un alfabet (nevid) oarecare, atunci luînd $M = (X^*, j, \wedge)$ se obține o structură de monoid complet ordonat pe mulțimea $\mathbf{p}(X^*)$ a limbajelor peste X, relativ la produsul de limbaje. Vom vedea (lema 4) că acesta din urmă este un monoid complet ordonat liber generat de X, deoarece pentru orice monoid complet ordonat W, orice aplicație $X \to W$ se extinde la un morfism $\mathbf{p}(X^*) \to W$ de monoizi complet ordonați.

2) Pentru o mulțime oarecare S se poate considera monoidul $W = (\mathrm{Rel}\, S, \circ, 1_S)$ al relațiilor binare pe S. Înzestrat cu structura de latice completă dată de incluziune, W este un monoid complet ordonat, deoarece compunerea de relații este distributivă în raport cu reuniunile : dacă $\mathcal{A}$, $\mathcal{B}$ sînt colecții de relații binare pe S, atunci

$$\bigcup_{A \in \mathcal{A},\, B \in \mathcal{B}} A \circ B = \left(\bigcup_{A \in \mathcal{A}} A\right) \circ \left(\bigcup_{B \in \mathcal{B}} B\right).$$

3) Dacă L este o latice completă, atunci mulțimea $\mathcal{C}(L)$ a operatorilor continui $L \to L$ are o structură de monoid complet ordonat. Pentru orice mulțime S are loc un izomorfism de monoizi complet ordonați $\mathrm{Rel}\, S \rightleftarrows \mathcal{C}(\mathbf{p}(S))$, $\rho \mapsto \tilde{\rho}$, definit prin luarea imaginii directe.

4) Dăm acum un exemplu mai special de monoid complet ordonat, anume *mulțimea seturilor de calcule*. Fie S o mulțime (de stări). Numim *calcul în* S orice șir finit de stări $\{s_0, \ldots, s_m\}$. Două calcule $c = \{s_0, \ldots, s_m\}$, $c' = \{t_0, \ldots, t_n\}$ se numesc *compozabile* dacă $s_m = t_0$; în acest caz se definește calculul $c * c' = \{s_0, \ldots, s_m, t_1, \ldots, t_n\}$. Observăm că operația $*$ nu este o concatenare. Calculele constituie un concept categorial și nu unul monoidal (așa cum sînt cuvintele din S^*). Notăm cu $\mathcal{K}_S$ categoria avînd un singur obiect —S, morfismele fiind calculele în S iar compunerea definită prin $*$.

Mulțimea $\mathbf{p}(\mathcal{K}_S)$ a seturilor de calcule în S formează în mod natural un monoid complet ordonat. Mai general, pentru orice categorie mică avînd $\mathcal{M}$ ca mulțime de morfisme, $\mathbf{p}(\mathcal{M})$ este un monoid complet ordonat punînd $F \cdot G = \{fg \mid f, g \text{ compozabile}, f \in F, g \in G\}$ pentru orice $F, G \in \mathbf{p}(\mathcal{M})$.

Dacă W este un monoid complet ordonat, un element $r \in W$ se numește extensiv (resp. preidempotent) dacă $1 \leqslant r$ (resp. $r^2 \leqslant r$). Dacă r este extensiv și preidempotent, atunci $r \leqslant r^2$ și $r^2 \leqslant r$, deci $r^2 = r$, adică r este idempotent. Mulțimea elementelor extensive și preidempotente din W, notată $\mathrm{RT}(W)$ este o parte inf-completă a lui W. Se arată ușor că $\mathrm{RT}(W)$ este Δ-sup completă. Orice element $x \in W$ admite o închidere extensivă și preidempotentă x^*; anume $x^* = 1 \vee x \vee x^2 \vee \ldots$

Exemple. 1) Dacă $W = \mathfrak{p}(M)$, M fiind un monoid, atunci pentru orice $A \in W$, adică $A \subset M$, A^* este submonoidul generat de A.

2) Dacă L este o latice completă și $W = \mathcal{C}(L)$, atunci conform corolarului 2 al teoremei 4.5 pentru orice $\varphi \in W$, avem $\varphi^* = c_\varphi$.

Categorii complet ordonate

O categorie mică $\mathbf{C}$ cu proprietatea că mulțimile de morfisme sînt latici complete și că pentru orice obiecte a, b, c, oricare ar fi mulțimile de morfisme $F \subset \mathbf{C}(a, b)$, $G \subset \mathbf{C}(b, c)$, rezultă $\sup(FG) = (\sup F)(\sup G)$, se numește categorie *complet ordonată.*

Exemple. 1) Un monoid complet ordonat poate fi privit ca o categorie complet ordonată avînd un singur obiect; invers, într-o categorie complet ordonată $\mathbf{C}$, pentru orice obiect $a \in \mathrm{Ob}\,\mathbf{C}$, mulțimea $\mathbf{C}(a, a)$ a morfismelor $a \to a$ este un monoid complet ordonat.

2) Categoria **Rel** a mulțimilor ca obiecte și relațiilor binare (ca morfisme) este complet ordonată. Aceeași proprietate o are categoria laticilor complete (ca obiecte) și a aplicațiilor continui (ca morfisme).

Un functor $F : \mathbf{C} \to \mathbf{C}'$ între două categorii complet ordonate se numește *continuu* dacă $\forall a, b \in \mathrm{Ob}\,\mathbf{C}$ și $\mathcal{F} \subset C(a, b)$, avem $\sup F(\mathcal{F}) = F(\sup \mathcal{F})$. Așadar, alături de morfisme identice și compuneri, functorii continui conservă $\perp = \sup \emptyset$, $\vee$ și operația $*$ (definită în mulțimile de forma $\mathbf{C}(a, a)$ care sînt monoizi complet ordonați, punînd $w^* = \sup_{k \geqslant 0} w^k$ pentru orice $w \in \mathbf{C}(a, a)$).

Pornind de la o categorie oarecare $\mathbf{C}$, considerăm aceleași obiecte ca în $\mathbf{C}$ și morfismele $(a, \mathcal{F}, b) : a \to b$ $(a, b \in \mathrm{Ob}\,\mathbf{C})$, unde $\mathcal{F} \subset \mathbf{C}(a\,b)$; compunerea fiind $(b, \mathcal{G}, c) \circ (a, \mathcal{F}, b) = (a, \mathcal{G} \circ \mathcal{F}, c)$, identitățile $(a, \{1_a\}, a)$ și ordinea $(a, \mathcal{F}, b) \leqslant (a, \mathcal{F}', b) \leftrightarrow \mathcal{F} \subset \mathcal{F}'$. În acest mod se obține o categorie complet ordonată notată $\mathbf{p(C)}$. Identificînd $f : a \to b$ cu $(a, \{f\}, b)$, $\mathbf{C}$ poate fi privită ca o subcategorie a lui $\mathbf{p(C)}$. Se poate demonstra următoarea proprietate de universalitate: pentru orice

categorie complet ordonată $\mathbf{Q}$, orice functor $F : \mathbf{C} \to \mathbf{Q}$ are o extensie, unică, la un functor continuu $\overline{F} : \mathbf{p(C)} \to \mathbf{Q}$. Anume, punem $\overline{F}(a) = F(a)$ și $\overline{F}(a, \mathcal{F}, b) = \sup F(\mathcal{F})$; pentru unicitate, observăm că $(a, \mathcal{F}, b) = \sup_{f \in \mathcal{F}} (a, \{f\}, b)$.

§ 4.5. O GENERALIZARE A TEOREMEI LUI KLEENE. APLICAȚII ÎN PROGRAMARE

Fie W un monoid complet ordonat și $\Sigma \subset W$ o submulțime fixată.

DEFINIȚIA 4.8. Numim Σ-*automat* (generalizare a definiției 3.12) un 4-uplu

$$\mathcal{A} = (Q, I, T, E),$$

unde Q este o mulțime finită de *stări* (de control), $I \subset Q$ o mulțime de *stări inițiale*, $T \subset Q$ o mulțime de *stări terminale* și $E \subset Q \times \Sigma \times Q$ o mulțime finită (eventual vidă) de *arce*.

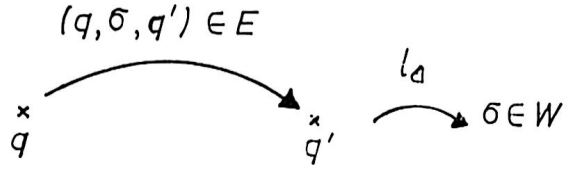


Fig. 4.3

Elementele lui E pot fi privite ca arce etichetate ale unui graf orientat $G_{\mathcal{A}}$ ale cărui noduri sînt stările din Q (fig. 4.3). Extindem funcția de etichetare

$$l_{\mathcal{A}} : E \to W, \quad (q, \sigma, q') \mapsto \sigma$$

la *toate* drumurile din graful $G_{\mathcal{A}}$. Pentru aceasta punem $l_{\mathcal{A}}(1_q) = 1$, unde 1_q este drumul nul $q \to q$ și $l_{\mathcal{A}}(pp') = l_{\mathcal{A}}(p) \cdot l_{\mathcal{A}}(p')$, unde pp' este compunerea (concatenarea) drumurilor p și p', iar produsul din membrul secund este efectuat în W.

Un drum $q \to q'$ în $G_{\mathcal{A}}$ se numește *reușit* dacă $q \in I$ și $q' \in T$. *Comportarea* lui $\mathcal{A}$ este elementul din W definit prin

$$|\mathcal{A}| = \sup l_{\mathcal{A}}\{\text{toate drumurile reușite în } G_{\mathcal{A}}\}.$$

Un element $w \in W$ se numește Σ-*recognoscibil* dacă există un Σ-automat $\mathcal{A}$ astfel încît $w = |\mathcal{A}|$. Vom nota cu $\mathrm{Rec}(\Sigma)$ mulțimea tuturor elementelor Σ-recognoscibile din W.

Pe de altă parte, să considerăm următoarea signatură (Ω, ν), $\nu : \Omega \to \mathbb{N}$, în sensul definiției 3.8 : $\Omega = \{\bot, 1, \vee, \cdot, *\}$; $\nu(\bot) = \nu(1) = 0$; $\nu(\vee) = \nu(\cdot) = 2$ și $\nu(*) = 1$.

Așadar, $\bot$ și 1 sînt simboluri de operații nulare, $\vee$ și $\cdot$ simboluri de operații binare, iar $*$ un simbol de operație unară.

Înzestrăm W cu o structură de Ω-algebră definind operațiile corespunzătoare în modul următor :

1) $\bot = \inf W$;

2) 1 este unitatea lui W ;

3) $\forall\, w, w' \in W, w \vee w' = \sup\{w, w'\}$;

4) $\cdot$ este produsul din W ;

5) $*$ este operația „star" a lui Kleene, deci

$$w^* = \sup\{w^k \mid k \in \mathbb{N}\} \quad (w^0 = 1\,;\ w^{k+1} = w \cdot w^k).$$

Aceste operații se mai numesc *operații raționale* pe W. Remarcăm că orice morfism de monoizi complet ordonați este un morfism de Ω-algebre.

Vom nota cu $\mathrm{Rat}(\Sigma)$ Ω-subalgebra lui W generată de Σ. Elementele lui $\mathrm{Rat}(\Sigma)$ sînt numite Σ-*raționale*; acestea sînt tocmai elementele din Σ sau sînt obținute din elementele din Σ aplicînd într-un număr finit de pași operații raționale.

Teorema Kleene

Rezultatul fundamental al acestui capitol îl constituie următoarea teoremă care generalizează la monoizi complet ordonați teorema lui Kleene și Schutzenberger ([24], [47]) regăsită în cazul monoidului limbajelor peste un alfabet finit A (luînd $W = \mathfrak{P}(A^*)$ și $\Sigma = A$).

Teorema 4.9 ([7]). *Dacă* $(W, \cdot, 1)$ *este un monoid complet ordonat, atunci pentru orice* $\Sigma \subset W$ *avem*

$$\mathrm{Rec}(\Sigma) = \mathrm{Rat}(\Sigma).$$

Demonstrația acestei teoreme necesită mai multe pregătiri și etape. Ideea de bază constă în a înlocui argumentele combinatorii prin unele algebrice; un punct important constă în faptul că mulțimile de drumuri din graful unui automat formează un monoid complet ordonat, iar funcția de etichetare poate fi extinsă la un morfism de monoizi complet ordonați.

Observație. În general, dacă $\mathfrak{M}$ este mulțimea morfismelor unei categorii mici, atunci $\mathfrak{p}(\mathfrak{M})$ este un monoid complet ordonat relativ la incluziune, cu produsul

$$AB = \{ab \mid a \in A, b \in B, a \text{ și } b \text{ compozabile}\}; \text{ am pus } ab = b \circ a.$$

Ca unitate am luat mulțimea tuturor morfismelor identice. Pe de altă parte, dacă W este monoid complet ordonat, atunci în exemplele care succed definiția 3.4 am definit categoria cu un singur obiect $\{W\}$ și având mulțimea morfismelor W. Dacă $f : \mathfrak{M} \to W$ este componenta pe morfisme a unui functor, atunci aplicația $\bar{f} : \mathfrak{p}(\mathfrak{M}) \to W$, $A \mapsto \sup f(A)$ este un morfism de monoizi complet ordonați (aplicînd proprietatea de universalitate a lui $\mathfrak{p}(X)$ din § 4.1).

Fie acum un monoid complet ordonat W, o submulțime $\Sigma \subset W$ și $\mathcal{A} = (Q, I, T, E)$ un Σ-automat. Notăm cu $G_{\mathcal{A}}^{\#} = \mathbf{d}(G_{\mathcal{A}})$ categoria având ca obiecte nodurile din $G_{\mathcal{A}}$ și ca morfisme toate drumurile din $G_{\mathcal{A}}$ (§ 3.1). Funcția de etichetare extinsă poate fi considerată ca un functor $l_{\mathcal{A}} : G_{\mathcal{A}}^{\#} \to W$ (conform teoremei 3.1 $G_{\mathcal{A}}^{\#}$ este categoria liber generată de $G_{\mathcal{A}}$, iar extinderea lui $l_{\mathcal{A}}$ decurge din proprietatea respectivă de universalitate; apoi W este privit ca o categorie cu un singur obiect). Vom nota mulțimea morfismelor din $G_{\mathcal{A}}^{\#}$ tot cu $G_{\mathcal{A}}^{\#}$. Conform observației anterioare, va rezulta un functor continuu $l_{\mathcal{A}} : \mathfrak{p}(G_{\mathcal{A}}^{\#}) \to W$ și un morfism de monoizi complet ordonați

$$\bar{l}_{\mathcal{A}} : \mathfrak{p}(G_{\mathcal{A}}^{\#}) \to W, \quad D \mapsto \sup\, l_{\mathcal{A}}(D).$$

Dacă pentru orice $A, B \subset Q$ notăm cu $[A \to B]_{\mathcal{A}}$ mulțimea tuturor drumurilor în $G_{\mathcal{A}}$ care încep într-o stare din A și se termină într-o stare B, atunci avem $|\mathcal{A}| = \sup\{l_{\mathcal{A}}(d) \mid d \in [I \to T]_{\mathcal{A}}\} = \bar{l}_{\mathcal{A}}[I \to T]_{\mathcal{A}}$.

În cazul clasic $W = \mathbf{p}(\Sigma^*)$, $\Sigma \subset W$; identificînd o literă $\sigma \in \Sigma$ cu limbajul $\{\sigma\} \in W$ și punînd pe aree limbaje, un Σ-automat pornește de la niște limbaje de bază care îi etichetează arcele și recunoaște un limbaj mai complicat obținut prin înmulțirea limbajelor de bază de-a lungul drumurilor și apoi reunindu-le pentru toate drumurile reușite. Aplicînd același tratament și clasei limbajelor ce se obțin prin operații raționale pornind de la limbaje de bază arbitrare, se obține o identitate a celor două clase de limbaje $\mathrm{Rec}(\Sigma)$ și $\mathrm{Rat}(\Sigma)$. Aceeași idee stă la baza generalizării enunțate, mulată pe exploatarea structurii de monoid complet ordonat.

Demonstrația teoremei

Fixăm deci un monoid complet ordonat W, o parte $\Sigma \subset W$ și notăm $\Sigma' = \Sigma \cup \{1\}$.

Etapa I-a. Arătăm că $\mathrm{Rat}(\Sigma) \subset \mathrm{Rec}(\Sigma')$.

Mai întîi să observăm că $\Sigma \subset \mathrm{Rec}(\Sigma')$, deoarece orice $\sigma \in \Sigma$ este comportarea Σ'-automatului $(\{i, t\}, i, t, (i, \sigma, t))$, $i \neq t$ [Am scris pe scurt i în loc de $\{i\}$, t în loc de $\{t\}$, convenție pe care o folosim și în continuare.]

Deoarece $\perp (= \sup \emptyset)$ este comportarea Σ'-automatului $(\emptyset, \emptyset, \emptyset, \emptyset)$, iar 1 este comportarea Σ'-automatului $(u, u, u, \emptyset)$, rezultă că $\perp, 1 \in \mathrm{Rec}(\Sigma')$.

Arătăm acum că $\mathrm{Rec}(\Sigma')$ este închisă (adică stabilă) relativ la operațiile $\vee$ și $.$. Fie deci $w_1, w_2 \in \mathrm{Rec}(\Sigma')$ și $\mathcal{A}_1 = (Q_1, I_1, T_1, E_1)$, $\mathcal{A}_2 = (Q_2, I_2, T_2, E_2)$ două Σ'-automate astfel încît $w_1 = |\mathcal{A}_1|$, $w_2 = |\mathcal{A}_2|$. Putem presupune fără a restrînge generalitatea că $Q_1 \cap Q_2 = \emptyset$ (înlocuind $\mathcal{A}_2$ printr-un automat izomorf cu el). Considerăm Σ'-automatul

$$\mathcal{A} = (Q_1 \cup Q_2, I_1 \cup I_2, T_1 \cup T_2, E_1 \cup E_2).$$

În mod evident, $[I_1 \cup I_2 \to T_1 \cup T_2]_{\mathcal{A}} = [I_1 \to T_1]_{\mathcal{A}} \cup [I_2 \to T_2]_{\mathcal{A}}$ și aplicînd funcția continuă $\bar{l}_{\mathcal{A}}$, rezultă $|\mathcal{A}| = \bar{l}_{\mathcal{A}}[I_1 \to T_1]_{\mathcal{A}} \vee \bar{l}_{\mathcal{A}}[I_2 \to T_2]_{\mathcal{A}}$. Deoarece există o corespondență bijectivă (conservînd etichetele) între mulțimile de drumuri $[I_1 \to T_1]_{\mathcal{A}}$ și $[I_1 \to T_1]_{\mathcal{A}_1}$, rezultă $\bar{l}_{\mathcal{A}}[I_1 \to T_1]_{\mathcal{A}} = |\mathcal{A}_1|$. În mod similar, $\bar{l}_{\mathcal{A}}[I_2 \to T_2]_{\mathcal{A}} = |\mathcal{A}_2|$ și ca atare $|\mathcal{A}| = |\mathcal{A}_1| \vee |\mathcal{A}_2|$, adică $w_1 \vee w_2 = |\mathcal{A}|$, deci $w_1 \vee w_2 \in \mathrm{Rec}(\Sigma')$.

Considerăm acum automatul

$$\mathcal{B} = (Q_1 \cup Q_2, I_1, T_2, E),$$

unde $E = E_1 \cup E_2 \cup \{(t_1, 1, i_2) | t_1 \in T_1, i_2 \in I_2\}$.

Este evident că

$$[I_1 \to T_2]_{\mathcal{B}} = [I_1 \to T_1]_{\mathcal{B}} \cdot \{(t_1, 1, i_2) | t_1 \in T_1, i_2 \in I_2\} \cdot [I_2 \to T_2]_{\mathcal{B}}.$$

Aplicînd $\bar{l}_{\mathcal{A}}$ rezultă ca mai înainte că $|\mathcal{B}| = |\mathcal{A}_1| \cdot |\mathcal{A}_2|$, deoarece $\bar{l}_{\mathcal{A}}\{(t_1, 1, i_2) | t_1 \in T_1, i_2 \in I_2\} = 1$. Așadar, $w_1 \cdot w_2 = |\mathcal{B}|$, adică $w_1 \cdot w_2 \in \mathrm{Rec}(\Sigma')$.

Rămîne să arătăm că $\mathrm{Rec}(\Sigma')$ este stabilă la operația „star". Fie $w \in \mathrm{Rec}(\Sigma')$ și un Σ'-automat $\mathcal{A} = (Q, I, T, E)$ astfel ca $w = |\mathcal{A}|$. Definim automatul

$$\mathcal{A}' = (Q \cup u, u, u, E'),$$

unde $E' = E \cup \{(u, 1, i) | i \in I\} \cup \{(t, 1, u) | t \in T\}$, presupunînd că elementul u nu aparţine lui Q (fig. 4.4). Să notăm cu $[I \to T]'_{\mathcal{A}'}$ mulţi-

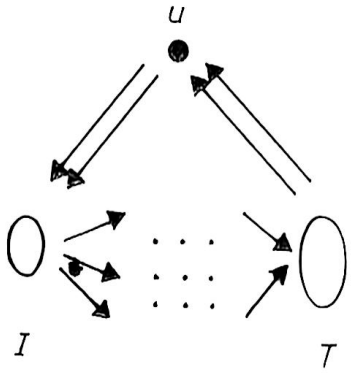


Fig. 4.4

mea tuturor drumurilor din $[I \to T]_{\mathcal{A}'}$ care nu trec prin u. În mod evident, $[u \to u]_{\mathcal{A}'} = (\{(u, 1, i) | i \in I\} \cdot [I \to T]'_{\mathcal{A}'} \cdot \{(t, 1, u) | t \in T\})^*$. Aplicînd $\bar{l}_{\mathcal{A}'}$ şi utilizînd un argument similar unuia anterior, rezultă $\bar{l}_{\mathcal{A}'}[I \to T]'_{\mathcal{A}'} = |\mathcal{A}|$ şi ca atare ţinînd cont că $\bar{l}_{\mathcal{A}'}\{(u, 1, i) | i \in I\} = \bar{l}_{\mathcal{A}'}\{(t, 1, u) | t \in T\} = 1$, se obţine $|\mathcal{A}'| = |\mathcal{A}|^* = w^*$, deci $w^* \in \mathrm{Rec}\,(\Sigma')$.

Am demonstrat deci că $\mathrm{Rec}\,(\Sigma')$ conţine Σ, $\perp$, 1 şi este stabilă la $\vee$, $\cdot$, $*$, deci $\mathrm{Rec}\,(\Sigma')$ va conţine $\mathrm{Rat}\,(\Sigma)$.

Etapa a II-a. Arătăm că $\mathrm{Rec}\,(\Sigma') \subset \mathrm{Rec}\,(\Sigma)$.

Fie $\forall w \in \mathrm{Rec}\,(\Sigma')$ şi $\mathcal{A} = (Q, I, T, E)$ un Σ'-automat astfel ca $w = |\mathcal{A}|$. Notăm cu D_1 mulţimea tuturor drumurilor din graful $G_{\mathcal{A}}$ care sînt nule sau etichetate cu 1 pe arce. Fie apoi E' mulţimea tuturor tripletelor $(q, \sigma, q') \in Q \times \Sigma \times Q$ pentru care în $G_{\mathcal{A}}$ există un drum $q \to q'$ de forma $p(q'', \sigma, q''')p'$, unde p şi p' aparţin lui D_1 şi $(q'', \sigma, q''') \in E$. Dacă în D_1 există drumuri reuşite, atunci considerăm Σ-automatul $\mathcal{A}' = (Q \cup u, I \cup u, T \cup u, E')$, unde $u \notin Q$; în caz contrar, luăm $\mathcal{A}' = (Q, I, T, E')$.

Pentru orice drum reuşit s din $G_{\mathcal{A}}$ *există cel puţin un drum reuşit* s' *din* $G_{\mathcal{A}'}$ *avînd aceeaşi etichetare* [Într-adevăr, dacă $s \in D_1$, atunci luăm $s' = 1_u$, iar dacă $s \notin D_1$, atunci s admite o descompunere, nu neapărat unică, în factori de forma $p(q'', \sigma, q''')p'$, cu $p, p' \in P$ şi $\sigma \in \Sigma$, şi înlocuind fiecare factor $q \to q'$ de acest tip cu (q, σ, q') se obţine s']. Reciproc, *pentru orice drum reuşit* s' *din* $G_{\mathcal{A}'}$ *există cel puţin un drum reuşit* s *în* $G_{\mathcal{A}}$ *avînd aceeaşi etichetare* [Într-adevăr, dacă s' este trivial, atunci sau el coincide cu 1_u în care caz există un drum reuşit $s \in D_1$ sau $s' = 1_q$ cu $q \neq u$ şi atunci putem lua $s = s'$. Iar dacă s' nu este trivial, atunci înlocuim fiecare arc (q, σ, q') care apare în s' printr-unul din drumurile de forma $p(q'', \sigma, q''')p'$, cu $p, p' \in D_1$, $(q'', \sigma, q''') \in E$, ceea ce face ca (q, σ, q') să aparţină lui E' şi astfel se obţine s.]

Cele două afirmații demonstrate anterior arată că $|\mathcal{A}| = |\mathcal{A}'|$, deci w este comportarea unui Σ-automat, adică $w \in \mathrm{Rec}\,(\Sigma)$.

Etapa a III-a. Arătăm că are loc și incluziunea $\mathrm{Rec}\,(\Sigma) \subset \mathrm{Rat}\,(\Sigma)$. Fie $\forall\, w = |\mathcal{A}| \in \mathrm{Rec}(\Sigma)$, $\mathcal{A} = (Q, I, T, E)$ fiind un Σ-automat. Dacă $Q = \emptyset$, atunci $w = \perp$, deci $w \in \mathrm{Rat}\,(\Sigma)$. Putem deci presupune că mulțimea Q este nevidă și fără a micșora generalitatea, putem lua $Q = \{1, \ldots, n\}$. Pentru orice părți $A, B \subset Q$ și oricare ar fi $0 \leqslant k \leqslant n$, notăm cu D^k_{AB} mulțimea tuturor drumurilor din graful $G_{\mathcal{A}}$ care au inițialul într-o stare din A, terminalul conținut în B și trec numai prin stări intermediare cu indici $\leqslant k$. Să notăm

$$w^k_{AB} = \bar{l}_{\mathcal{A}}(D^k_{AB}) = \sup\{l_{\mathcal{A}}(D) \mid D \in D^k_{AB}\}.$$

Deoarece D^0_{AB} constă doar dintr-un număr finit (eventual vid) de drumuri triviale sau arce de lungime 1, se observă direct că $w^0_{AB} \in \mathrm{Rat}\,(\Sigma)$. [Dacă $a \to b$ este un drum din D^0_{AB} și dacă $a \neq b$, atunci $l_{\mathcal{A}}(a \to b) = \sup\{\sigma \mid (a, \sigma, b) \in E\}$, iar dacă $a = b$, atunci $l_{\mathcal{A}}(a \to b) = 1 \vee \vee \sup\{\sigma \mid (a, \sigma, a) \in E\}$; cum E este mulțime finită, rezultă că w^0_{AB} se exprimă utilizînd doar $\vee$, 1, $\perp$ și elementele din Σ.] Apoi, pentru orice $A, B \subset Q$ și pentru orice $1 \leqslant k \leqslant n$, orice drum din D^k_{AB} aparține sau lui D^{k-1}_{AB} sau este de forma

$$q \to k \to \ldots \to k \to q',$$

unde sînt indicate toate stările intermediare k. Prin urmare,

$$D^k_{AB} = D^{k-1}_{AB} \cup [D^{k-1}_{Ak} \cdot (D^{k-1}_{kk})^* \cdot D^{k-1}_{kB}].$$

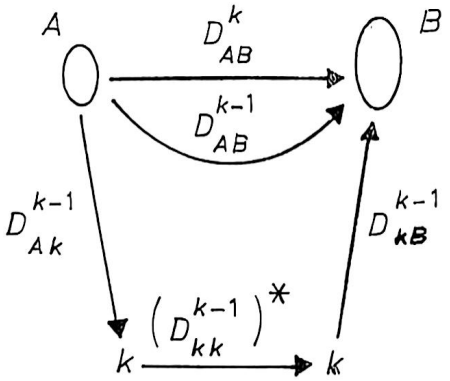


Fig. 4.5

Aplicînd funcția continuă $\bar{l}_{\mathcal{A}}$, se obține

$$w^k_{AB} = w^{k-1}_{AB} \vee [w^{k-1}_{Ak} \cdot (w^{k-1}_{kk})^* \cdot w^{k-1}_{kB}].$$

Prin inducție rezultă că $w^k_{AB} \in \mathrm{Rat}(\Sigma)$ pentru orice $A, B \subset Q$ și oricare ar fi $0 \leqslant k \leqslant n$. În particular, rezultă că $w = |\mathcal{A}| = w^n_{IT} \in \mathrm{Rat}(\Sigma)$ și cu aceasta etapa a III-a este parcursă.

Din incluziunile

$$\mathrm{Rat}(\Sigma) \subset \mathrm{Rec}(\Sigma') \subset \mathrm{Rec}(\Sigma) \subset \mathrm{Rat}(\Sigma),$$

rezultă că $\mathrm{Rec}(\Sigma) = \mathrm{Rat}(\Sigma)$ și teorema 4.9 este complet demonstrată. ∎

Cazul monoidului complet ordonat liber

În cele ce urmează, vom utiliza simultan mai mulți monoizi complet ordonați. De aceea dacă W este un monoid complet ordonat și $\Sigma \subset W$, atunci în loc de Σ-automat, $\mathrm{Rec}(\Sigma)$, $\mathrm{Rat}(\Sigma)$, vom scrie (W, Σ)-automat, $\mathrm{Rec}(W, \Sigma)$ și, respectiv, $\mathrm{Rat}(W, \Sigma)$.

LEMA 4. *Pentru orice mulțime X, $\mathbf{p}(X^*)$ este un monoid complet ordonat liber generat de X.*

Demonstrație. Considerăm aplicația $i : X \to \mathbf{p}(X^*)$, $x \mapsto \{x\}$. Avem deci de arătat că pentru orice monoid complet ordonat W și pentru orice aplicație de mulțimi $f : X \to W$, există și este unic un morfism de monoizi complet ordonați $F : \mathbf{p}(X^*) \to W$ astfel încît $F \circ i = f$. Într-adevăr, notînd cu $f^* : X^* \to W$ unica extindere a lui f la un morfism de monoizi (teorema 1.7), aplicăm proprietatea de universalitate a lui $\mathbf{p}(X^*)$ demonstrată la p. 164. Atunci, există și este unică o aplicație continuă $F : \mathbf{p}(X^*) \to W$ astfel încît $F(\{c\}) = f^*(c)$ pentru orice cuvînt $c \in X^*$; anume $F(A) = \sup\{f^*(L) \mid L \subset A \subset X^*\}$. Această aplicație este un morfism de monoizi complet ordonați.

LEMA 5. *Dacă $h : W \to W'$ este un morfism de monoizi complet ordonați și $\Sigma \subset W$, atunci*

$$h(\mathrm{Rat}(W, \Sigma)) = \mathrm{Rat}(W', h(\Sigma)).$$

Demonstrație. Folosind signatura (Ω, ν) legată de operațiile raționale 1) — 5) definite anterior, am remarcat că h este un morfism de Ω-algebre și lema rezultă evident printr-un raționament simplu de algebră universală.

LEMA 6. *Fie $h : W \to W'$ un morfism de monoizi complet ordonați, $\Sigma \subset W$ și $\mathcal{A} = (Q, I, T, E)$ un (W, Σ)-automat. Considerăm $(W', h(\Sigma))$-automatul*

$$h(\mathcal{A}) = (Q, I, T, h(E)),$$

unde $h(E) = \{(q, h(\sigma), q') \mid (q, \sigma, q') \in E\}$. *Atunci*

$$|h(\mathcal{A})| = h(|\mathcal{A}|).$$

Demonstrație. Fie $h_G : G_{\mathcal{A}} \to G_{h(\mathcal{A})}$ morfismul de grafuri definit prin $h_G(q) = q$ și $h_G(q, \sigma, q') = (q, h(\sigma), q')$. Notăm cu $h_G^{\#} : G_{\mathcal{A}}^{\#} \to G_{h(\mathcal{A})}^{\#}$ unica extindere a lui h_G la un functor între categoriile libere corespunzătoare (conform teoremei 3.1). Acest functor este bijectiv pe obiecte și, în plus, $h_G^{\#}[I \to T]_{\mathcal{A}} = [I \to T]_{h(\mathcal{A})}$. Mai mult, se verifică ușor că $h \circ l_{\mathcal{A}} = l_{h(\mathcal{A})} \circ h_G^{\#}$ și un calcul simplu arată că $h(|\mathcal{A}|) = |h(\mathcal{A})|$. ∎

TEOREMA 4.10. *Dacă W este un monoid complet ordonat și $\Sigma \subset W$ și dacă* $\mathrm{Rec}(\mathbf{p}(\Sigma^*), \Sigma) = \mathrm{Rat}(\mathbf{p}(\Sigma^*), \Sigma)$, *atunci* $\mathrm{Rec}(W, \Sigma) = \mathrm{Rat}(W, \Sigma)$.

Demonstrație. Conform lemei 4 rezultă (pentru $X = \Sigma$) că incluziunea $j : \Sigma \to W$, $\sigma \mapsto \sigma$, admite o extindere unică la un morfism de monoizi complet ordonați $J : \mathbf{p}(\Sigma^*) \to W$ și observăm că $J(\Sigma) = \Sigma$. Conform lemei 5 rezultă $\mathrm{Rat}(W, \Sigma) = J(\mathrm{Rat}(\mathbf{p}(\Sigma^*), \Sigma))$. Aplicînd apoi lema 6, rezultă incluziunea $\mathrm{Rec}(W, \Sigma) \supset J(\mathrm{Rec}(\mathbf{p}(\Sigma)^*, \Sigma))$.

Rămîne să demonstrăm incluziunea

$$\mathrm{Rec}(W, \Sigma) \subset J(\mathrm{Rec}(\mathbf{p}(\Sigma^*), \Sigma)).$$

Pentru aceasta fie $\mathcal{A} = (Q, I, T, E)$ un (W, Σ)-automat. Notăm prin $\mathcal{A}^* = (Q, I, T, E)$, $(\mathbf{p}(\Sigma^*), \Sigma)$-automatul în care elementele lui Σ sînt privite ca litere ale unui alfabet (și nu ca elemente din W). Cu notațiile din lema 6 și aplicînd rezultatul din lema 6 avem $\mathcal{A} = J(\mathcal{A}^*)$ și $|\mathcal{A}| = J(|\mathcal{A}^*|)$, rezultă imediat incluziunea dorită. ∎

În demonstrațiile clasice ale teoremei originale a lui Kleene condiția ca mulțimea Σ să fie finită poate fi înlocuită prin finitudinea mulțimii arcelor (ca în definiția 4.8). Atunci teorema 4.9 se poate deduce din teorema clasică a lui Kleene și din teorema 4.10. Demonstrația dată mai sus pentru teorema 4.9 în cazul mai general al monoizilor complet ordonați este esențialmente aceeași ca în cazul unui monoid complet ordionat liber.

Aplicații în programare

a) Am dat mai sus o generalizare a teoremei lui Kleene care acoperă o arie mai largă decît cea a limbajelor peste un alfabet. Aplicînd teorema 4.9 monoidului relațiilor binare peste o mulțime, obținem echivalența computațională între două doctrine privind construcția de programe. În prima programele sînt organigrame generale,

de fapt grafuri etichetate cu comenzi și în cea de a doua, programele sînt construite în același mod cu expresiile raționale.

Trecem la precizarea acestor afirmații. Fie S o mulțime ale cărei elemente le numim *stări de informație*. Notăm cu $W = (\mathrm{Rel}\, S, \circ, 1_S)$ monoidul complet ordonat al relațiilor binare pe S (definiția 4.7). Elementele din W se vor numi *transformări de stare peste* S (nedeterministe, atît timp cît relațiile din W nu sînt funcționale). Fie apoi $\Sigma \subset \mathrm{Rel}\, S$ o submulțime, ale cărei elemente vor fi numite *transformări de bază*. Σ-automatele (definiția 4.8) vor fi numite *programe-organigramă* (*nedeterministe peste* Σ).

Se poate spune că am fixat setul de instrucțiuni sau comenzi pentru o mașină abstractă iar Σ-automatele constituie un model pentru programe de tip organigramă pentru această mașină abstractă. Stările unui Σ-automat sînt numite *stări de control* spre deosebire de stările lui S care sînt stări de informație ale mașinii abstracte.

Dacă $\mathcal{A}$ este un program-organigramă, atunci comportarea $w = |\mathcal{A}| \in W$ este o relație binară pe S, numită *relația calculată prin programul* $\mathcal{A}$.

Se pornește cu o stare inițială de informație $s_0 \in S$ dintr-o stare inițială de control i și se parcurge un drum reușit în graful programului, aplicînd pentru fiecare arc traversat transformarea de stare care îl etichetează. În acest caz, $\mathrm{Rec}(\Sigma)$ este tocmai mulțimea transformărilor de stare „calculabile" cu ajutorul programelor-organigramă peste Σ.

Să considerăm acum Ω-algebra Σ^Ω generată de Σ, unde $\Omega = \{\bot, 1, \cdot, \vee, *\}$ este signatura considerată la punctul anterior. Elementele ei, numite și expresii raționale, sînt termeni „bine formați" construiți din operații cu simboluri din Ω efectuate asupra transformărilor de bază și vor fi numite *programe raționale peste* Σ (*nedeterministe*).

Așadar, pornind de la elementele lui Σ se definesc expresii raționale $r \in \Sigma^\Omega$; printre acestea notăm: orice $\sigma \in \Sigma$, $\bot$, 1 și $e \cdot e'$, $e \vee e'$, e^* ori de cîte ori $e, e' \in \Sigma$. Expresiile raționale joacă rolul de programe structurate. Analogia cu programarea structurată uzuală este următoarea: $\bot$ = instrucțiunea *buclează*; 1 = instrucțiunea *continuă*; $\cdot$ = construcție secvențială, $\vee$ = construcție alternativă, $*$ = construcție repetitivă.

Mulțimea programelor raționale peste Σ fiind o Ω-algebră liber generată de Σ, rezultă că pentru incluziunea $j : \Sigma \hookrightarrow W$, există și este unic un morfism $J : \Sigma^\Omega \to W$ de Ω-algebre astfel încît $J|\Sigma = j$. În plus, $\mathrm{Rat}(\Sigma) = \{J(r) \mid r \in \Sigma^\Omega\}$, adică $\mathrm{Rat}(\Sigma)$ este mulțimea transformărilor de stare calculabile prin expresii raționale. Așadar, incluziunea $\Sigma \subset \mathrm{Rel}\, S$ are o extindere unică la un morfism de Ω-algebre

J, care *asociază oricărui program rațional relația calculată de el* (se mai spune că J este semantica).

Pentru $W = \mathrm{Rel}\, S$, din teorema 4.9 se deduce direct următorul rezultat remarcabil.

TEOREMA 4.11. *Programele raționale calculează exact aceleași relații ca și programele-organigramă.* ■

Din considerațiile anterioare, rezultă că programarea prin programe raționale este un analog nedeterminist al programării structurate deterministe. Deci programarea structurată este „rațională"!

b) Să notăm cu C o mulțime ale cărei elemente vor fi numite *simboluri de comenzi*. Numim *C-mașină* orice pereche (S, φ), unde S este mulțimea stărilor de informație ale mașinii și $\varphi : C \to \mathrm{Rel}\, S$ este o aplicație (sau interpretare). Pentru orice simbol de comandă $c \in C$, mașina „interpretează" acest simbol într-o relație binară pe S, adică o transformare de stare $\varphi(c) : S \to S$, nedeterministă.

Numim *C-schemă program* pentru C-mașina (S, φ) orice $\varphi(C)$-automat în sensul definiției 4.8 pentru $W = \mathrm{Rel}\, S$ (cu structura naturală de monoid complet ordonat). Comportarea unui astfel de automat poate fi numită *transformarea de stare* calculată de el. Să notăm cu $C^{(p)}$ mulțimea tuturor $\varphi(C)$-automatelor; orice element din $C^{(p)}$ se poate identifica printr-un element din $\mathbf{p}(C^*)$. Atunci funcția $\varphi : C \to \mathrm{Rel}\, S$ se poate extinde la o funcție $\overline{\varphi} : C^{(p)} \to \mathrm{Rel}\, S$. Pentru orice $\varphi(C)$-automat $\gamma \in C^{(p)}$ notăm cu $\varphi^{(p)}(\gamma)$ comportarea automatului (obținută înlocuind simbolurile de comenzi prin interpretările lor).

Considerăm signatura $\Omega = \left\{ \begin{matrix} 0 & 0 & 2 & 2 & 1 \\ \bot, & 1, & \cdot, & \vee, & * \end{matrix} \right\}$ explicitată la p. 188, cu aritățile respective. Se numește *C-schemă rațională* orice element al Ω-algebrei $C^{(r)}$ generată de C.

Dacă avem o C-mașină (S, φ), atunci observăm că pe $\mathrm{Rel}\, S$ există o structură de Ω-algebră (se definesc respectiv relația vidă, relația identică, compunerea de relații, reuniunea și închiderea reflexivă și tranzitivă. Aplicația $\varphi : C \to \mathrm{Rel}\, S$ se extinde atunci la o aplicație $\varphi^{(r)} : C^{(r)} \to \mathrm{Rel}\, S$.

Noțiunile de C-schemă de program și C-schemă rațională (C fiind o mulțime de simboluri de comenzi) pot fi generalizate înlocuind C-mașina printr-un monoid complet ordonat W, împreună cu o aplicație de interpretare $\varphi : C \to W$. Un rol special îl are „interpretarea liberă", obținută luînd pentru W monoidul complet ordonat liber generat de C, adică $W = \mathbf{p}(C^*)$ și $i : C \to \mathbf{p}(C^*)$, $c \mapsto \{c\}$. Pentru orice altă interpretare $\varphi : C \to W$, există și este unic un morfism de monoizi complet ordonați $\overline{\varphi} : \mathbf{p}(C^*) \to W$ astfel ca $\overline{\varphi} \circ i = \varphi$.

Deoarece orice monoid complet ordonat W este o Ω-algebră, rezultă totodată că interpretarea $\varphi : C \to W$ are o extindere rațională

$\varphi^{(r)} : C^{(r)} \to W$. Se verifică uşor că $\varphi^{(r)} = \overline{\varphi} \circ i^{(r)}$ şi *dacă două C-scheme raţionale coincid în interpretarea liberă, atunci ele coincid în orice altă interpretare.* Un rezultat similar are loc şi pentru C-scheme program. Anume, avem $\overline{\varphi} \circ i^{(p)} = \varphi^{(p)}$; într-adevăr, $\forall\, \gamma \in C^{(p)}$, $\varphi^{(p)}(\gamma) = |\overline{\varphi}(\gamma)| \overset{\text{lema 6}}{=} \overline{\varphi}(|\gamma|)$ şi cum $\bar{i} = 1$ rezultă $i^{(p)}(\gamma) = |\bar{i}(\gamma)| = |\gamma|$.

Se poate de asemenea extinde un rezultat al lui Herbrand: *dacă două scheme program* (resp. *raţionale*) *coincid în orice monoid complet ordonat de tipul* Rel S (S *fiind o mulţime oarecare*), *atunci ele coincid în orice alt monoid complet ordonat* (acest rezultat aparţine lui D. Suciu).

Într-adevăr, să observăm mai întîi că pentru orice monoid M există un morfism injectiv de monoizi complet ordonaţi

$$\alpha : \mathbf{p}(M) \to \text{Rel}\, M,\ A \subset M \mapsto \{(m, am) \mid m \in M,\ a \in A\}.$$

Fie deci γ_1, γ_2 două C-scheme program şi $M = C^*$. Conform ipotezei avem $\overline{(\alpha \circ i)}^{(p)}(\gamma_1) = \overline{(\alpha \circ i)}^{(p)}(\gamma_2)$. Dar, în general, $\varphi^{(p)} = \overline{\varphi} \circ i^{(p)}$, deci $\overline{(\alpha \circ i)} \circ i^{(p)}(\gamma_1) = \overline{(\alpha \circ i)}(i^{(p)}(\gamma_2))$ şi, cum $\overline{(\alpha \circ i)} = \alpha$ iar α este injectiv, rezultă $i^{(p)}(\gamma_1) = i^{(p)}(\gamma_2)$. Atunci pentru orice interpretare $\psi : C \to W$ avem $\overline{\psi} \circ i^{(p)} = \psi^{(p)}$, deci $\psi^{(p)}(\gamma_1) = \psi^{(p)}(\gamma_2)$. În mod similar se procedează pentru cazul cînd γ_1, γ_2 sînt C-scheme raţionale.

Aceste consideraţii arată legătura strînsă între cele două filozofii de programare — organigramele şi programele raţionale.

BIBLIOGRAFIE

1. M. Arbib, A. J. Kfoury, R. N. Moll, *A basis for theoretical computer science*, Springer Verlag, Berlin, 1981.
2. D. W. Barnes, J. M. Mack, *An algebraic introduction to mathematical logic*, Springer Verlag, Berlin, 1975.
3. Ş. Basarab, V. Nica, D. Popescu, *Aproximation properties and existential completeness for ring morphisms*, Manuscripta Math. **33** (1981), 227—282.
4. C. Bănică, O. Stănăşilă, *Spectrul unei latici*, Stud. Cerc. Mat. **19**,1 (1967), 137—145.
5. G. Birkoff, Th. C. Bartee, *Modern applied algebra*, Mc. Graw Hill, New York, 1971.
6. W. S. Brainerd, L. H. Landweber, *Theory of computation*, J. Wiley, New York, 1974.
7. V. Breazu, O. Stănăşilă, *A generalization of Kleene's theorem and nondeterministic structured programing*, Information and Control **51**, 2, (1981), 146—152; *Overtopologies and their algebraic significance*, Bul. I.P.B., **43**, 3 (1981), 3—10.
8. V. Brînzănescu, *Capitole de matematici speciale* (note de curs), Lit. I.P.B. 1978.
9. I. Bucur, *Capitole speciale de algebră*, Ed. Academiei R.S.R, Bucureşti, 1980.
10. F. Bucur, *Obiecte înzestrate cu o structură aritmetică într-o categorie arbitrară*, Stud. Cerc. Mat. **23**, 2 (1971), 181—184.
11. C. Calude, *Complexitatea calculului*, Ed. Ştiinţifică şi Enciclopedică, Bucureşti, 1982.
12. V. Căzănescu, *Curs de scheme de programare, latici continue*, Lit. Univ. Bucureşti, 1980; *Introducere în teoria limbajelor formale*, Ed. Academiei R.S.R., Bucureşti, 1983.
13. S. Eilenberg, *Automata, Languages and Machines*, vol.A, Academic Press, New York, 1974.
14. A. Filipoiu, *Polinoame şi algebre de polinoame cu mai multe sorturi*, Bul. I.P.B., **14**, 2 (1978), 7—15.
15. P. Flondor, *An example of a fuzzy system*, Kybernetics, **6** (1977).
16. Gh. Galbură, *Algebră*, Ed. Didactică şi Pedagogică, Bucureşti, 1972.
17. Cr. Giumale, E. Kalisz, *Structura datelor şi tehnici de programare*, Lit. I.P.B., 1981.
18. V. M. Gluškov, G. E. Ţeitlin, E. L. Iuschenko, *Algebra iazîki programirovanie*, Naukova Dumka, Kiev, 1978.
19. I. D. Ion, C. Niţă, *Elemente de aritmetică cu aplicaţii în tehnici de calcul*, Ed. Tehnică, Bucureşti, 1978.
20. I. D. Ion, N. Radu, *Algebra*, Ed. Didactică şi Pedagogică, Bucureşti, 1981.
21. Tr. Ionescu, *Sisteme şi echipamente pentru conducerea sistemelor*, Ed. Didactică şi Pedagogică, Bucureşti, 1982.
22. Vl. Ionescu, C. Popeea, *Optimizarea sistemelor*, Ed. Didactică şi Pedagogică, Bucureşti, 1981.
23. N. Jacobson, *Basic Algebra* I, Freeman, San Francisco, 1974.
24. S. C. Kleene, *Reprezentation of events in nerve sets and finite automate*, Automata studies, Ann. Math. Studies **34**, (1956), Princeton.

25. F. W. Lawvere, *An elementary theory of the category of sets*, Proc. Nat. Acad. Sci. U.S.A. **51** (1964), 1506—1510.
26. P. E. Liepa, W. M. Wonham, *Feedback systems in a general algebraic setting*, IEEE Trans. on Circuits and Systems, CAS—25, **9** (1978), 728—741.
27. L. Livovski, C. Popovici, H. Georgescu, N. Ţăndăreanu, *Bazele informaticii*, Ed. Didactică şi Pedagogică, Bucureşti, 1981.
28. A. Lustig, *Redirecţionarea codului dirijată prin tabele*, Lucrările simpozionului Info-Iaşi, 1982.
29. I. Manin, *Mathematical Logic*, Springer Verlag, Berlin, 1981.
30. S. Marcus, *Algebraic Linguistic; analytical models*, Academic Press, New York, 1967; *Lingvistica matematică*, Ed. Didactică şi Pedagogică, Bucureşti, 1973; *Gîndirea algoritmică*, Ed. Tehnică, Bucureşti, 1983.
31. F. Moldoveanu, *Contribuţii la optimizarea proiectării produselor program* (teza de doctorat), 1982.
32. M. Moroianu, *Teoremele lui Zorn-Bourbaki şi aplicaţii ale lor*, Bul. I.P.B.,**17**, 3 (1980), 9—14.
33. A. Niţă, *Quellques observations sur les ultraproduits d'anneaux*, Bull. Math. Soc. Sci. Math. R. S. Roumanie **20**, 3—4 (1976), 325—328.
34. Gh. Păun, *Noi operaţii cu limbaje*, Stud. Cerc. Mat. **29**, 5 (1977), 521—533; *Mecanisme generative ale proceselor economice*, Ed. Tehnică, Bucureşti, 1982.
35. A. Petrescu, *Microprogramare*, Ed. Tehnică, Bucureşti, 1975; *Microcalculatoare Felix* M18, M18B, M118 (în colab.) vol. I, II, Ed. Tehnică, Bucureşti, 1984.
36. M. Petrescu, *Analiza şi sinteza dispozitivelor numerice* (note de curs), Lit. I.P.B., 1982.
37. C. Popa, *Semantic definition of the concept of method*, Rev. de Sci. Social.; Phil. Logiq. **23**, 3—4 (1979), 371—383; *Logica acţiunii*, Ed. Ştiinţifică şi Enciclopedică, Bucureşti, 1983.
38. C. Popa, O. Stănăşilă, *Asupra sistemelor de norme* (în vol. *Logica acţiunii*, Ed. Ştiinţifică şi Enciclopedică, Bucureşti, 1983, pp. 73—83).
39. N. Popescu, *Abelian categories with applications*, Academic Press, New York, 1973.
40. N. Răbâncă, A. Taşcă, A. Truică, *Clasificarea dinamicilor evolutive*, Bul. I.P.B.(va apărea).
41. M. Reghiş, *Elemente de teoria mulţimilor şi de logică matematică*, Ed. Facla, Timişoara, 1981.
42. S. Rudeanu, *Boolean functions and equations*, North-Holland, London, New York, 1974; *Curs de bazele informaticii*, Lit. Univ. Bucureşti, 1982.
43. I. Rus, *Principii şi aplicaţii ale teoriei punctului fix*, Ed. Dacia, Cluj-Napoca, 1979.
44. T. Rus, *Data structures and operating systems*, J. Wiley, Londra, 1979.
45. Gr. Sabău, O. Stănăşilă, *Capitole de matematică aplicată*, note de curs, 1983.
46. A. Salomaa, M. Soittola, *Automata theoretic aspects of formal power series*, Springer Verlag, Berlin, 1978.
47. M. P. Schützenberger, *On the definition of a family of automata*, Information and Control **4** (1961), 247—270.
48. D. Scott, *Continuous lattices*, Lecture Notes in Math. **274** (1972), 97—136.
49. D. Stanomir, O. Stănăşilă, *Metode matematice în teoria semnalelor*, Ed. Tehnică, Bucureşti, 1980.
50. O. Stănăşilă, *Elemente de matematică discretă* (note de curs), Lit. I.P.B., 1978; *Analiză matematică*, Ed. Didactică şi Pedagogică, Bucureşti, 1981; *Scop şi construcţie* (în vol. *Logica acţiunii*, Ed. Ştiinţifică şi Enciclopedică, Bucureşti 1983, pp. 50—56); *Sistem formal şi logică deontică* (în vol. *Praxiologie şi logică*, Ed. Academiei R.S.R., Bucureşti, 1984).
51. T. Stihi, *Logică matemctică* (note de curs), Lit. I.P.B., 1980.
52. D. Suciu, *Asupra unei teoreme de izomorfism în algebre universale*, Bul. I.P.B. 2, (1983), 15—17.
53. L. Şerbănaţi, *Teoria automatelor*, Lit. I.P.B., Bucureşti, 1975.

54. Cr. Tănăsescu, *O tehnică de definire a modelelor pentru memorie*, Bul. I.P.B., Ser. Elth. **24**, 2 (1982), 98—104.
55. J. W. Thatcher, E. G. Wagner, J. B. Wright, *Notes on algebraic fundamentals for theoretical computer science*, IBM Thomas J. Watson Research Center **109** (1979), 83—163.
56. I. Tomescu, *Introduction to Combinatorics*, Collet's, London and Wellirghorough, 1975; *Teoria grafurilor*, Lit. Univ. Bucureşti, 1980; *Probleme de combinatorică şi teoria grafurilor*, Ed. Didactică şi Pedagogic, Bucureşti, 1981.
57. J. F. Tremblay, R. Manohar, *Discrete mathematical structures with applications to computer sciences*, Mc. Graw Hill, New York, 1975.
58. D. Vaida, *Algoritmi de compilare*, Ed. Didactică şi Pedagogică, Bucureşti, 1971; *Elemente de teoria limbajelor de programare* (formalizarea sintaxei şi semanticii), Lit. Univ. Bucureşti, 1973.
59. G. Burstein, P. Flondor, V. Ionescu, *Sisteme neliniare*, Lit. I. P. B., 1985.
60. M. Fliess, *Fonctionelles causales non linéaires et indeterminées non comutatives*, Bull. Soc. Math. France, **109**, 3—40 (1981).
61. St. Niculescu, *Iniţiere în programare structurată*, Ed. Tehnică, Bucureşti, 1979.
62. M. Tîrnoveanu, *Sicteme deontic-aletice transfinite de ordin zero*, Ed. ştiinţifică şi Enciclopedică, Bucureşti, 1983.
63. A. M. Turing. *Computing machinery and intelligence*, The world of math., tom 4, 1956 (433—460).

INDICE DE NOȚIUNI

alfabet 45
algebră Boole 128
algebră de propoziții 126
— ITE 129
algoritm 145
aplicație 14
— continuă 162
— de evaluare 34
— izotonă 17, 160—162
arbore 112, 131
— etichetat 133
— ordonat 132
automat-arbore 141
automat-finit 99
— în sens Eilenberg 136
— redus 101
— vid 137
axioma alegerii 84
— infinitului 83

C-mașină 196
C-schemă program 196
C-schemă rațională 196
calcul 144—145, 185,
caracteristica unui corp 105
cateoria categoriilor 196
categorie 115
— complet ordonată 186
circuit logic 129
cod binar 9
configurație instantanee 95
concatenare 45, 48, 137
congruență 162
cuplaj în paralel 19
— în serie 19
cuvînt 45
cuvînt vid 38, 45
cuvinte acceptate 138
cuvinte binare 38
— de lungime n 38

dinamica automatului 99
— Peano 22
dinamică 21
— evolutivă 36
dinamici algebric izomorfe 30
— cu inițializare 22
dicționarul unui alfabet 45
dinamomorfism 21
drum 112, 137
— închis 112
— nul 112, 137
— reușit 137, 146, 188

element idempotent 99
— izolat 177
— maximal 17
— minimal 17
— primitiv 107
element Σ-recognoscibil 188
eticheta operației algebrice 41

functor 119
— continuu 186
— identic 119
— ștergător 119
funcția de comportare 101
— de ieșire 99
— de luare a imaginii directe 173
— de stare-ieșire 141
— nulă 148
— produs 149
— sumă 149
funcție de etichetare 137
— de intrare 113
— de selecție 84

— generatoare 67
— necalculabilă 147
— parţială 14, 40
— periodică 102
— totală 14, 40, 145
funcţii LOOP calculabile 155, 161
— parţial recursive 149
— primitiv recursive 149

graf 109
— conex 113
— etichetat 113
grafic 11
gramatică 151
grup 43
— ciclic 103
— simetric 103

indice 15
inel 44
inducţie monoidală 52
— succesivă 54
izomorfism de grupuri 44
— de latici 130
— de monoizi 44

lanţ 17, 113
latice 128
— booleană 128
— distributivă 128
latici algebrice 170
— complete 161
— topologice 170
limbaj 46
limbaj recognoscibil 139
limbajul LOOP 150
litere 45

majorant 41
maşina LOOP 161
maşina Turing 97
minorant 41
monoid ciclic 97
— complet ordonat 181
— comutativ 41
— liber 48
monoidul unui automat 100
monoizi echidivizibili 60
morfism de dinamici 21
— de grafuri 111
— cu iniţializare 22
— de monoizi 42
— de semiinele 45
— identic de dinamici 21

multiport electric 40
mulţimea seturilor de calcule 185
mulţime cît 40
— finită 78
— infinită 84
— majorată 17
— minorată 17
— ordonată 17
— ordonată Z-completă 160
— vagă 89
— vidă 9

n-port 41
numărare 92
— canonică 93
numărul lui Gödel 97

obiect iniţial 118
— terminal 118
operator de închidere 165
operator izoton 166
operaţie algebrică 15
— n-ară 41
— nulară 41
— unară 41
operaţii raţionale 188
ordin de aritate 40
ordinea lexicografică 93

parte inf-completă 165
— p-completă 165
polinom caracteristic 69
— ireductibil 106
— reductibil 106
predicat binar 16
— generalizat 89
— n-ar 40
— nular 40
principiul lui Dirichlet 86
produs cartezian 10, 38
program-organigramă 195
proiecţii canonice 15
punct fix 178
puterea continuului 88

relaţie 11
— binară 11
— de aritate 38
— de derivare 151
— de compatibilitate 16
— de echivalenţă 16
— de ordine 16
— parţială 16

— funcţională 13
— totală 13
— vidă 38
— recursiv primitivă 148
reprezentarea zecimală 33

scheme logice 114
serie constantă 63
— nulă 63
— formală de puteri 63
signatură 122
simbolul vid (blanc) (94)
simboluri de comenzi 196
sistem de închidere 168
— — algebrică 170
— — topologică 170
— de intrare ieşire 19
— discret 182
— iterativ 144
stare iniţială 96, 144
stare terminală 96, 144
stări de control 195
— de informaţie 195
— indiscernabile 184
succesor 132
suport 63
Σ-algebră 122
Σ-automat 114
Σ-organigramă 114
— accesibilă 118

teorema lui Fermat 104
teorema lui Kleene 188
teorema lui Knäster-Tarski 178
teza lui Church 147, 149
transformări de bază 195
— de stare 196

X-automat 136
X-semiautomat 136

Redactor: MARIA BORICEAN
Tehnoredactor: OLIMPIU POPA

Coli de tipar 13
Bun de tipar 12.08.1985

c. 126 — I. P. INFORMAȚIA
str. Brezoianu nr. 23—25
București

Lei 16,50